

**PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION**

Before the

MARYLAND TASK FORCE TO STUDY IDENTITY THEFT

on

Combating Identity Theft: Implementing a Coordinated Plan

Annapolis, Maryland

September 18, 2007

I. INTRODUCTION

Senator Kelley, Delegate Lee, and members of the Task Force, I am Betsy Broder, Assistant Director of the Federal Trade Commission's Division of Privacy and Identity Protection ("FTC" or "Commission").¹ I appreciate the opportunity to speak about the FTC's role in protecting consumers from identity theft through law enforcement, consumer and business education; our coordination with state and local governments; and implementation of the recommendations from the President's Identity Theft Task Force. I also applaud your efforts to help Maryland residents avoid the serious consequences of this information-age crime.

Identity theft takes a devastating toll on its victims, our economy, and consumers' overall sense of on-line safety. Controlling it, therefore, is a critical component of the Commission's consumer protection mission. This testimony describes the nature and scope of the identity theft problem, actions the FTC has taken to combat identity theft, and the initiatives launched through the President's Identity Theft Task Force.

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. For example, in a Zogby Interactive poll

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.

earlier this year, 91% of adults surveyed were concerned that their identities might be stolen, over half of whom were “very concerned.”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.⁵ Public entities, including federal, state and local governments,

³ See Zogby Poll: *Most Americans Worried About Identity Theft*, available at www.zogby.com/search/ReadNews.dbm?ID=1275. See also 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 actually forgive the \$50 and will not hold the consumer 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 within 60 days of receiving the bank statement that lists such debits, they may be subject to unlimited liability for losses that occurred after that period. *Id.*

⁵ See, e.g., Darrell Smith, *Apology sent over CalPERS privacy error*, Sacramento Bee, August 27, 2007, at A14 (California state pension fund places Social Security numbers of hundreds of thousands of retirees on address labels); Ellen Nakashima, *U.S. Exposed Personal Data*, Washington Post, April 21, 2007, at A05 (United States Department of Agriculture displays the SSNs of over 60,000 grant recipients on public web page); Nick Shields, *Computer Containing Personal Data Stolen*, Baltimore Sun, April 25, 2007 (Baltimore County Department of Health has laptop containing personal

collect personal information about individuals for a variety of purposes, such as determining who is eligible for government programs. Accordingly, public entities play a critical role in guarding against misuse and unauthorized disclosure of the personal information they collect and maintain.

III. FTC ACTIONS TO COMBAT IDENTITY THEFT

Federal, state, and local governments must work together to reduce the opportunities for thieves to obtain consumers' personal information, and make it more difficult for thieves to misuse the information if they do obtain it. The FTC plays a central role in this endeavor through its own efforts as well as through coordination with industry, states, and consumer groups.

A. Law Enforcement on Data Security

One important way to keep sensitive information out of the hands of identity thieves is by ensuring that those who maintain such information adequately protect it. To further that goal, the Commission brings law enforcement actions against businesses that fail to implement reasonable security measures to protect sensitive consumer data.

Public awareness of, and concerns about, data security continue at a high level as reports about breaches of sensitive personal information proliferate.⁶ Recent breaches have touched both

information of approximately 6,000 patients stolen); *FEMA Statement on the Inadvertent Breach of Private Information*, available at www.fema.gov/media/archives/2007/042007.shtm (Federal Emergency Management Agency includes SSNs of 2,300 employees on address labels); *Secretary of State Recovers Thousands of 'Active' Fulton County Voter Registration Cards*, available at www.sos.state.ga.us/pressrel/20070411a.htm (75,000 Fulton County, Georgia voter registration cards, which include name, address, and SSN, recovered from trash container).

⁶ See, e.g., Jennifer Skalka, *MDE Reports Stolen Laptop*, Baltimore Sun, August 30, 2007 (Maryland Department of Environment reports theft of laptop containing SSNs of 10,000 Maryland residents); Dennis O'Brien, *Second Hospital Reports Lost Data*, Baltimore Sun, February 13, 2007 (hospital reports laptop containing information of 130,000 patients stolen); Rachel Sams, *Mercantile Says Laptop Theft Could Put Customers at Risk*, Baltimore Business Journal, May 12, 2006 (laptop containing information of 48,000 customers stolen from bank).

the public and private sectors. Of course, not all data breaches lead to identity theft; in fact, most breaches have not resulted in detected incidents of identity theft.⁷ Nonetheless, some breaches - especially those that result from deliberate actions by criminals, such as hacking - have led to identity theft.⁸

The FTC enforces several laws that establish requirements for the protection of covered data. The Commission's Safeguards Rule under the Gramm-Leach-Bliley Act ("GLB Act"), for example, contains data security requirements for financial institutions.⁹ The Fair Credit Reporting Act ("FCRA") includes certain due diligence requirements for consumer reporting agencies¹⁰ and safe disposal obligations for entities that maintain consumer report information.¹¹ State attorneys general can enforce the FCRA in instances where a federal agency has not already filed an action.¹² In addition, the FTC has enforced the Federal Trade Commission Act's

⁷ See Government Accountability Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), available at www.gao.gov/new.items/d07737.pdf.

⁸ See, e.g., n17, *infra*.

⁹ 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.

¹⁰ 15 U.S.C. § 1681 *et seq.* The FCRA specifies that consumer reporting agencies may provide consumer reports only for enumerated "permissible purposes," and requires that they have reasonable procedures to verify the identity and permissible purposes of prospective recipients of their reports.

¹¹ The FTC's implementing disposal rule is at 16 C.F.R. Part 382.

¹² See 15 U.S.C. § 1681s (c).

proscription against unfair or deceptive acts or practices¹³ where a business made false or misleading claims about its security procedures, or where its failure to employ reasonable security procedures caused substantial consumer injury.¹⁴

Since 2001, the Commission has brought fourteen cases challenging businesses that allegedly failed to reasonably protect sensitive consumer information that they maintained.¹⁵ In a number of these cases, the Commission alleged that the company had misrepresented the nature or extent of its security procedures in violation of the FTC Act's prohibition on deceptive practices.¹⁶ In addition, in several of the cases, the Commission alleged that the security inadequacies led to breaches that caused substantial consumer injury and were thus unfair practices under the FTC Act.¹⁷ Some of the cases involved enforcement of the Commission's GLB Act Safeguards Rule or the FCRA.¹⁸

¹³ 15 U.S.C. § 45(a).

¹⁴ See, e.g., *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006).

¹⁵ See generally <http://www.ftc.gov/privacy/index.html>.

¹⁶ E.g., *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.), *supra*, note 14; *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).

¹⁷ E.g., *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.), *supra*, note 14; *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (March 7, 2006); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005).

¹⁸ E.g., *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.), *supra*, note 14; *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of*

Probably the best-known FTC data security case was its action against ChoicePoint, Inc. ChoicePoint, a data broker, inadvertently sold sensitive information (including credit reports in some instances) on more than 160,000 consumers to a criminal gang, which in some cases used that information to commit identity theft. The Commission alleged that ChoicePoint failed to use reasonable procedures to screen prospective purchasers of its information. For example, 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. In settling the case, ChoicePoint agreed to pay \$10 million in civil penalties for violations of the FCRA and \$5 million in consumer redress for identity theft victims, and agreed to undertake substantial new data security measures.¹⁹

Although the Commission has brought its data security cases under different laws, the cases share common elements: the company's alleged security vulnerabilities were multiple and systemic, and readily-available and often inexpensive measures were available to prevent them. Together, the cases stand for the proposition that companies should maintain reasonable and appropriate measures to protect sensitive consumer information.

The FTC Safeguards Rule promulgated under the GLB Act serves as a good model of this approach. Firms covered by the Rule must prepare a written plan; designate an official with

Superior Mortgage Corp., FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of Nationwide Mortgage Group Inc.*, FTC Docket No. 9319 (April 15, 2005); *In the Matter of Sunbelt Lending Services*, FTC Docket No. C-4129 (Jan. 3, 2005).

¹⁹ See FTC News Release, *ChoicePoint Settles Data Security Breach Charges: To Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress* (Jan. 26, 2006), available at <http://www.ftc.gov/opa/2006/01/choicepoint.shtm>. The Commission has mailed more than 2,400 claims forms to possible victims and has created a website where consumers can download claims forms and obtain information about the claims process.

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 specifies 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.²⁰ This standard recognizes that there cannot be "perfect" security, and that data breaches can occur despite the maintenance of reasonable precautions to prevent them. It also is a flexible and adaptable standard that accounts for the fact 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" principles in enforcing existing data security laws.

B. The FACT Act

The 2003 Fair and Accurate Credit Transactions Act ("FACT Act") added a number of new provisions to the FCRA, which were intended to reduce the incidence of identity theft or minimize the injury to victims. First, with respect to prevention, the FACT Act contains provisions to limit the opportunities for wrongdoers to obtain unauthorized access to sensitive information. For example, the Act mandates that businesses dispose of consumer report

²⁰ Maryland has taken a similar approach towards data security enforcement in the recently adopted "Personal Information Protection Act," which requires businesses to maintain "reasonable security procedures and practices that are appropriate to the nature of the personal information owned . . . and the nature and size of the business and its operations." 2007 Maryland Laws Ch. 532 (H.B. 208).

information in a safe manner.²¹ Also, merchants must truncate the account number and redact the expiration date on consumers' copies of electronic credit card receipts.²²

Second, the FACT Act increases consumers' opportunities to review their credit records and spot incipient signs of identity theft before further damage ensues. Consumers have the right to receive a free credit report every twelve months,²³ through a centralized source, from each of the nationwide consumer reporting agencies ("CRAs"), as well as from nationwide "specialty" CRAs.²⁴

Third, the FACT Act empowers consumers to take steps to limit the damage from identity theft if they become victims. 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 report to exercise special

²¹ 15 U.S.C. § 1681w.

²² *Id.* at § 1681c(g).

²³ Maryland law allows its residents to obtain an additional free credit report from each of the nationwide CRAs. *See* 15 U.S.C. § 1681t (exempting Maryland's consumer report law from the FCRA's general preemption provision).

²⁴ *Id.* at § 15 U.S.C. § 1681j(a)(1)(C). The Commission has acted aggressively to uphold the integrity of the free report program, including bringing two actions against a company that offered "free" credit reports tied to the purchase of a credit monitoring service, through the website www.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 original case in 2005, the Commission charged, among other things, that the defendants, affiliates of the nationwide consumer reporting agency Experian, had deceptively mimicked the FACT Act free report program. The stipulated order required the defendants to make prominent disclosures that their program is not associated with the free annual report program and provide a link to the official website for that program, www.annualcreditreport.com. The defendants also agreed to disgorge \$950,000, 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 prohibits the company from suggesting that it is affiliated with the FACT Act program, and includes a \$300,000 judgment for consumer redress.

vigilance in opening accounts in the consumers' names.²⁵ Actual victims may request an extended, seven-year alert if they provide a police report to the CRA.²⁶ In addition, victims may obtain from creditors the underlying documentation associated with transactions that may have been fraudulent,²⁷ have the consumer reporting agencies block fraudulent information on their credit file,²⁸ and prohibit creditors from reporting fraudulent information to CRAs.²⁹

C. Consumer and Business Education

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. Through its online complaint form and toll-free hotline, the Commission receives approximately 15,000 to 20,000 contacts each week from consumers who obtain advice on how to recover from identity theft, or how to avoid becoming a victim in the first place. The FTC's identity theft primer³⁰ and victim recovery guide³¹ are widely available in print and online. Since 2000, the Commission

²⁵ 15 U.S.C. § 1681c-1(a).

²⁶ *Id. at* § 1681c-1(b).

²⁷ *Id. at* § 1681g(e).

²⁸ *Id. at* § 1681c-2.

²⁹ *Id. at* § 1681s-2(a)(6).

³⁰ *Avoid ID Theft: Deter, Detect, Defend*, available at <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt01.htm>.

³¹ *Take Charge: Fighting Back Against Identity Theft*, available at <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.htm>.

has distributed a total of 7 million copies of the two publications, and recorded over 3.7 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 legislators to educate their employees, communities, and constituencies. The Commission has distributed over 2.6 million brochures and 55,000 kits to date, and has recorded more than 3.2 million visits to the education program’s website 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 recently initiated an outreach campaign to place FTC educational materials on subway cars in New York, Chicago, San Francisco, and Washington D.C.

The Commission also sponsors a multimedia website, www.onguardonline.gov, designed to educate consumers about basic computer security, including the importance of not disclosing personal information to possible fraudsters.³² OnGuard Online was developed in partnership with other government agencies and the technology sector, and since its launch has attracted more than 4.3 million visits.

The Commission directs its outreach to businesses as well. The FTC recently released a new business guide on data security. The guide articulates the key steps that businesses should take as part of a sound data security plan:

³² See <http://www.onguardonline.gov/index.html>.

- “Take stock” - Know what personal information you have in your files and on your computers,
- “Scale down” - Keep only what you need for your business,
- “Lock it” - Protect the information that you keep,
- “Pitch it” - Properly dispose of what you no longer need, and
- “Plan ahead” - Create a plan to respond to security incidents.

D. Identity Theft Data Clearinghouse

The FTC also maintains the Identity Theft Data Clearinghouse, a national identity theft victim complaint database containing over a million complaints. Although the FTC itself does not have criminal prosecutorial authority, it does support criminal law enforcement by making these complaints available to federal, state, and local law enforcement agencies nationwide, including over 20 agencies in Maryland alone.³³ Law enforcers with access to the Clearinghouse can search the database for victims’ names or addresses, the police department that took the report, the type of offense involved, the companies involved, and suspect information. In addition to helping law enforcement generate leads in investigations, the Clearinghouse also enables agencies to link reports of identity theft that might otherwise have appeared to be isolated incidents. The Clearinghouse also gives information about the agencies involved in investigating a case, enabling law enforcement to coordinate their efforts and avoid duplication of efforts.

III. PRESIDENT’S IDENTITY THEFT TASK FORCE

On May 10, 2006, the President issued an Executive Order, establishing an Identity Theft Task Force, comprised of 17 federal agencies and co-chaired by the Attorney General and FTC

³³ See <http://www.consumer.gov/sentinel/members.htm>.

Chairman Deborah Platt Majoras, with the mission of developing a comprehensive national strategy to combat identity theft.³⁴ 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.

In April 2007, the Task Force published its strategic plan for combating identity theft.³⁵ 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 identity, 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 recommends 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

³⁴ Exec. Order No. 13,402, 71 FR 27945 (May 10, 2006).

³⁵ The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* ("Strategic Plan"), available at <http://www.idtheft.gov>.

the key item of information that identity thieves need. The Plan also recommends that the Task Force work with state and local governments – through organizations such as the National Governor’s Association and the National Association of Attorneys General – to highlight and discuss the vulnerabilities created by the use of SSNs and to explore ways to eliminate unnecessary use and display of SSNs.

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

In addition, the Plan recommends

- 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 uses 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 recommends a number of steps to aid those who assist victims, as well as the victims themselves. These include the development of easy-to-use reference materials for law enforcement and the implementation of a standard police report. The Report also recommends nationwide training for counselors at federal and state-sponsored victim assistance programs. The Department of Justice's Office for Victims of Crime has already begun offering workshops designed to train state, tribal, and local victim service providers.

The Report also recommends that the Task Force agencies examine certain tools that state and local governments have made available for identity theft victims. First, the Report recommends that the Task Force study the feasibility of developing a nationwide system that would allow identity theft victims to obtain identification documents that verify their identity, and thus avoid further victimization. As you know, Maryland has initiated such a "passport" system recently through the Motor Vehicle Administration. That program allows those drivers who can establish that they are identity theft victims to have a "V" placed on their license, which indicates that they are victims. Such programs are designed to prevent the misuse of the victim's name in the criminal justice system when, for example, an identity thief uses his victim's name when arrested. Recognizing the pioneering efforts of state governments in this area, the Report

specifically recommends that any nationwide program build on the programs developed by states, as well as a similar program established by the FBI.

The Report also recommends that the FTC assess state laws that grant consumers the right to place a credit freeze on their credit reports, making them inaccessible by creditors. Such laws are designed to prevent identity theft by blocking access to a consumer's credit report, thus making it nearly impossible for anyone to open a new credit account in the consumer's name. Over 30 states, including Maryland, have enacted such laws. The FTC will evaluate the effectiveness of such laws, as well as the costs they impose on consumers and businesses. The FTC will then prepare a report of its findings for use by policy makers in considering whether a federal credit freeze law would be appropriate.

In addition, the Plan recommends

- amending the federal criminal restitution statute to enable victims to recover for the value of their time spent in attempting to remedy the harms they suffered,
- developing an Identity Theft Victim Statement of Rights, and
- studying the impact and effectiveness of the victim remedies established under the FACT Act amendments to the Fair Credit Reporting Act.

3. Deterrence

The Plan includes a host of recommendations for strengthening law enforcement's ability to detect and punish identity thieves, including several aimed at providing assistance to state and local governments. For example, the Report recommends increasing the number of regional identity theft seminars, which are conducted by the FTC, federal investigative agencies, and the American Association of Motor Vehicle Administrators for state and local law enforcement

officers, and an increase of resources available for law enforcement available over the Internet. The report also recommends greater coordination among law enforcement agencies, and the development of federal/state task forces to address identity theft investigations and prosecutions. Some of the other major recommendations include:

- development of a national identity theft law enforcement center to better consolidate, analyze, and share identity theft information among law enforcers,
- enhanced tools to target off-shore identity thieves,
- diplomatic efforts to encourage other nations to clamp down on identity theft rings operating in their countries,
- expanded training of investigators and prosecutors,
- evaluation of current monetary thresholds for prosecution,
- several amendments to federal criminal statutes, and
- development of more precise data on the cost and prevalence of identity theft.

4. Status of Recommendations

Most of the Task Force recommendations have either already been implemented or are in the process of being implemented. For example, the Office of Management and Budget has issued data security and breach management guidance for government agencies.³⁶ The FTC has developed and distributed detailed data security guidance for businesses,³⁷ is planning regional

³⁶ OMB Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (May 22, 2007), *available at* <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf>; OMB Memorandum "Recommendations for Identity Theft Related Data Breach Notification" (Sept. 20, 2006), *available at* http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf.

³⁷ See <http://www.ftc.gov/infosecurity/>.

data security conferences, has conducted a workshop on consumer authentication,³⁸ has published an identity theft victim statement of rights on its website and at www.idtheft.gov, and is leading the interagency study of the private sector usage of Social Security numbers. The Department of Justice has forwarded to Congress a set of legislative recommendations that seek to close existing loopholes for the prosecution of some types of identity theft,³⁹ and is developing and presenting expanded training for their prosecutors and, in partnership with the FTC, for state and local law enforcement. As noted earlier, Task Force agencies also are examining several programs that were initiated at the state level, including laws that enable consumers to freeze their credit reports and “passport” programs that help identity theft victims prove their identity.

III. CONCLUSION

Identity theft remains a serious problem in our society, causing enormous harm to consumers and businesses and threatening consumer confidence in the marketplace. The Federal Trade Commission has attacked this problem aggressively through its law enforcement actions, its participation on the Identity Theft Task Force, and its extensive consumer and business education and outreach efforts. To succeed in the battle against identity theft, federal, state, and local governments, working together with the private sector, must make it more difficult for thieves to obtain the information they need to steal identities, make it more difficult to use that information if they do obtain it, and assist victims when thefts occur. The Commission will continue to partner and coordinate with state and local governments in the ongoing fight against identity theft.

³⁸ See <http://www.ftc.gov/bcp/workshops/proofpositive/index.shtml>.

³⁹ See http://www.usdoj.gov/opa/pr/2007/July/07_crt_522%20%20%20.html.