# The Federal Trade Commission

**Remarks of Chairman Deborah Platt Majoras**[1]
**Teaming Up Against Identity Theft: A Summit on Solutions**
**Los Angeles, CA**
**February 23, 2006**

**"Teamwork: The Key to Victory Against Identity Theft"**

## I.Introduction

Thank you. I am pleased to be here for California's second summit on identity theft. I thank Charlene Zettel, Director of the California Department of Consumer Affairs for inviting me, and I applaud the state's leadership in this area. The state of California and the Federal Trade Commission share a common goal and a clear commitment to identity theft prevention and victim assistance.

Identity theft is a particularly pernicious crime requiring swift action on many fronts. Like a virus, it spreads through our economic system, striking randomly and often inflicting great harm on innocent victims. According to a San Jose, California consumer who called the FTC's consumer help line, in just one day identity thieves opened nine credit card accounts in her name and incurred $15,000 in charges. Unfortunately, this victim's tale is not unusual – and it is far from the most egregious case.

[1] The views expressed herein are my own and do not necessarily represent the views of the Federal Trade Commission or of any other Commissioner.

The theme for today's Summit is "teaming up" and that is perfect. Vince Lombardi, America's "prophet" on teamwork, said "people who work together will win, whether it be against complex football defenses, or the problems of modern society." In an era when it is fashionable to categorize issues as federal, state, or local, identity theft stands out as genuinely requiring a coordinated response at all levels. Officials at all levels of government, the private sector, and consumers all play critical roles in this fight, and the whole is greater than the sum of its parts. As Mr. Lombardi said: "Individual commitment to a group effort – that is what makes a team work, a company work, a society work . . . ."

**II.The Role of Government**

State and local officials, district attorneys, and police departments provide the offense. They are the primary players in tracking down and prosecuting identity thieves and in providing their victims with assistance in reclaiming their identities, and their experience provides invaluable insights to all who work together to solve this difficult problem. While these are sometimes complex cases to investigate and prosecute, criminal law enforcement authorities are persevering and putting these thieves behind bars where they belong. One such thief who we will not be hearing from for a long time is Mr. Oluwatosin, who was just sentenced to 10 years imprisonment and ordered to make restitution of $6 million as part of the ongoing criminal investigation involving data broker ChoicePoint.[2] This case, which was investigated by the Los

[2] *See* Los Angeles County District Attorney's Office press release "Nigerian Gets 10 Years Prison; Must Pay $6.5 Million in Identity Theft Case" (Feb. 10, 2006), *available at http://da.co.la.ca.us/mr/021006a.htm?zoom_highlight=+Oluwatosin.*

Angeles County District Attorney's Office and Sheriff's Department, as well as several federal agencies, is a prime example of successful teamwork.

State and local agencies also provide the first helping hand to victims, who often turn first to their local police departments or state consumer protection agencies for assistance. State and local governments are especially well-positioned for this role because they can provide their residents with victim assistance that is tailored to their needs.

Because state and local government are on the front line, they also have been innovators in developing new ideas for tackling identity theft. The California law requiring consumer notice after certain types of data breaches, for example, has raised awareness about the issue of data security, and brought about important changes.

## III.The Role of the Federal Trade Commission

The federal government also is playing a strong role in the fight against identity theft. At the FTC, we take seriously our responsibility to promote a coordinated framework for attacking a national problem; vigorously enforce consumer protection laws related to identity theft and data security; assist criminal law enforcement authorities in bringing identity thieves to justice; assist victims in recovery; and educate consumers and businesses.

### A.FTC Enforcement

Americans' concerns about the security of their personal data and their risk of identity theft have spiked with recent reports about data breaches. The FTC's aggressive law enforcement program, using our full arsenal of statutory tools, targets companies that fail to implement reasonable measures to protect sensitive consumer information.

One of the FTC's most recent law enforcement actions arose from ChoicePoint's high-profile breach that occurred last year and was reported pursuant to California law. In our complaint, we allege that consumer data broker, ChoicePoint, Inc., failed to use reasonable procedures to screen prospective subscribers and monitor their access to sensitive consumer data, in violation of the Fair Credit Reporting Act (FCRA)[3] and the FTC Act.[4] For example, the company allegedly approved as customers individuals who lied about their credentials, used commercial mail drops as business addresses, and faxed multiple applications from nearby public commercial locations. According to our complaint, ChoicePoint's failures allowed identity thieves to obtain access to the personal information of over 160,000 consumers, including nearly 10,000 consumer reports, and to commit identity theft. The FTC alleged that at least 800 cases of identity theft arose out of these incidents. The Commission obtained $10 million in civil penalties for the FCRA violations – the highest civil penalty ever levied in a consumer protection case – $5 million in consumer redress for identity theft victims, and significant injunctive provisions that require Choicepoint to implement a variety of new data security measures. This settlement is an important victory for consumers and also an important lesson for industry.

The ChoicePoint settlement follows on a dozen security cases against household names like Microsoft, DSW Shoe Warehouse, BJ's Wholesale Club, and others. In some of these cases, we alleged that the companies made false promises to take reasonable steps to protect sensitive

---

[3] 15 U.S.C. §§ 1681-1681x.

[4] *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (complaint and proposed settlement filed on Jan. 30, 2006 and pending court approval).

consumer information.[5] In others, we alleged that the failure to take reasonable security measures to protect sensitive customer data was an unfair practice in violation of the FTC Act.[6] And in a third group of cases, we alleged violations of federal rules under the Gramm-Leach-Bliley Act (GLBA)[7] requiring "financial institutions" to implement safeguards for their data.[8] No matter what the source of our legal authority, these cases all stand for the proposition that record keepers must protect sensitive consumer information.

And just this morning, to reinforce that message, the Commission is announcing a settlement with CardSystems Solutions, Inc., the processor allegedly responsible for the Visa and MasterCard breach last year affecting tens of millions of credit and debit cards.[9] This case

---

[5] *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). Documents related to these enforcement actions are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

[6] *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. 042-3160 (Sept. 20, 2005); *In the Matter of DSW, Inc.*, FTC Docket No. 052-3096 (proposed settlement posted for public comment on Dec. 1, 2005). Documents related to the enforcement action against BJ's Wholesale Club are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html. Documents relating to the enforcement action against DSW are available at http://www.ftc.gov/os/caselist/0523096/0523096.htm.

[7] 15 U.S.C. § 6801-09.

[8] 15 U.S.C. § 6801(b); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 ("Safeguards Rule"). *In the Matter of Sunbelt Lending Services*, FTC Docket No. C-4129 (Jan. 3, 2005); *Nationwide Mortgage Group, Inc.*, FTC Docket No. 9319 (April 12, 2005); *Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005).

[9] *In the Matter of Card Systems Solutions, Inc. and Solidus Networks, Inc., d/b/a Pay by Touch Solutions*, 052-3148 (proposed settlement posted for public comment on Feb. 23, 2006).

addresses the largest known compromise of financial data to date. Here again, the FTC alleged that CardSystems engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive consumer data. The settlement requires CardSystems and its successor corporation to implement a comprehensive information security program and obtain audits by an independent third-party professional every other year for 20 years. As noted in the FTC's press release, CardSystems faces potential liability in the millions of dollars under bank procedures and in private litigation for losses related to the breach.

The ultimate goal here is not to rack up more settlements and fines. That is not how we will measure our success. Rather, the goal here is to create a culture of security for sensitive information so that businesses prevent breaches and identity theft. Our cases make plain that they first must implement reasonable data security practices to keep sensitive consumer data such as Social Security numbers from falling into criminal hands. The laws and rules we enforce do not require that information security be perfect. That would be a costly, unobtainable standard. Rather, we require that a company's data security be reasonable in light of the nature of its business and the sensitivity of the information it handles. That is "Data Security 101."

Consumer information is the currency of our information economy. Just as we know that businesses keep their cash safe, we must insist that they keep consumers' sensitive information safe.

In addition, businesses must implement strong fraud prevention measures to prevent identity thieves from using consumer information to perpetrate fraud. For example, by using strong authentication measures, a business can ensure that a person is who he or she purports to be, and thus spot and screen out potential identity thieves.

Many companies already have shown leadership on these fronts, and we applaud them. We also commend industry for working to assist identity theft victims through, for example, the Identity Theft Assistance Center, or ITAC as it is known, which was established by major banks to work one-on-one with victims to resolve their problems. Still, some companies have failed to implement even basic information security measures that can be implemented at relatively low cost, such as developing a security plan, training employees about data security issues, and overseeing service providers that have access to sensitive customer data. In our cases, for example, we alleged that some of the companies failed to defend against common, well-known Web attacks; some stored credit card data when they had no business need to do so; and some stored sensitive data in files that could be accessed easily by using commonly known default user IDs and passwords. The consent orders settling these cases require the companies to implement comprehensive information security programs and obtain third party audits.[10]

---

[10] In addition to our law enforcement efforts, we also have an active rulemaking program to implement provisions of the Fair and Accurate Credit Transactions Act of 2003, or FACT Act, related to identity theft. The FACT Act requires the FTC, alone or in conjunction with other agencies, to adopt 18 rules, undertake eight studies, and conduct three consumer education campaigns. To date, we have completed eleven rules or similar obligations, proposed two additional rules, published five studies, and completed one consumer education campaign with two others in progress.

In 2005, the FTC issued a final rule requiring businesses that make firm offers of credit or insurance to consumers, often called "prescreened offers," to provide enhanced disclosures of consumers' right to opt out of receiving such offers. 16 CFR 642 and 698 App. A (70 Fed. Reg. 5022; Jan. 31, 2005). *See* "FTC Prescreen Opt-out Notice Rule Takes Effect August 1" (July 27, 2005), *available at* http://www.ftc.gov/opa/2005/07/prescreenoptout.htm In addition, the FCRA requires all businesses and individuals who use consumer reports to take reasonable steps to dispose of the reports once they are done with them. 15 U.S.C. § 1681w. The purpose of this requirement, which is embodied in the so-called Disposal Rule, is to protect against unauthorized access to the reports, such as when identity thieves troll for sensitive information left in dumpsters. Perhaps most importantly, the FACT Act gives consumers nationwide the right to a free annual credit report. 15 U.S.C. § 1681j(a)(1).

Our FACT Act work is not yet done. The Commission is working with the bank regulatory agencies to develop the so-called "Red Flags" Rule that requires financial institutions

If the law enforcement message is not enough, companies must realize that inadequate security is just bad business. A Visa International survey of more than 6,000 consumers across 12 countries, conducted following some of the recent high-profile data breaches, found that data security was a major concern for 64% of respondents. The survey also found that consumers changed their behavior due to fears about identity theft, with 24% reporting that they limited use of online shopping sites.[11] Similarly, a survey by the Ponemon Institute found that, of the respondents who had received a letter notifying them of a data breach, 58% said it decreased their trust and confidence in the organization.[12] These surveys make clear that providing appropriate protections for sensitive consumer information is good business.

**B.FTC Outreach**

Outreach to and among businesses, consumers, and law enforcement is critical. The 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act") assigned the FTC a unique role in combating identity theft and coordinating government efforts.[13] Thus, in addition to law enforcement, the Commission's program includes business education to promote better security practices; consumer education and victim assistance; and coordination with other law

---

and creditors to spot signs of identity theft. 15 U.S.C. § 1681m.

[11] *See* Visa press release "Technology, Cross-industry Collaboration Key to Enhancing Security" (Jan. 25, 2006), *available at* http://corporate.visa.com/md/nr/press280.jsp?src=home.

[12] *See* Consumer Affairs press release "Data Breaches Bad for Business" (Sept. 27, 2005), *available at* http://www.consumeraffairs.com/news04/2005/data_breaches_business.html. Nineteen percent said they immediately terminated their accounts with vendors who lost the information; 40% considered taking their business elsewhere; and 5% said they hired lawyers.

[13] Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

enforcement through the Identity Theft Data Clearinghouse, a centralized database of victim complaints.

Our business outreach efforts include providing guidance on issues related to data security. For example, the Commission has disseminated guidance for businesses on reducing risks to their computer systems,[14] as well as guidance on complying with the GLBA Safeguards Rule.[15] We also have published *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, a business education brochure on managing data compromises.[16] This publication provides guidance on when it would be appropriate for an entity to notify law enforcement and consumers in the event of a breach of personal information.

Finally, the FTC operates the Identity Theft Data Clearinghouse, the nation's central database of victim complaints designed to support law enforcement investigations nationwide. The database includes over one million complaints received directly from consumers as well as various state and federal agencies. It enables us to gain a better understanding of how identity theft is afflicting consumers and serves as a resource for over 1,300 law enforcement agencies, more than 100 of which are California law enforcement agencies.

To encourage greater use of the Clearinghouse, the FTC staff offers seminars to law enforcement across the country. Teaming up with the Department of Justice, the U.S. Postal Inspection Service, FBI, the American Association of Motor Vehicle Administrators, and the U.S. Secret

---

[14] *See* Security Check: Reducing Risks to Your Computer Systems, *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/security.htm.

[15] *See* Financial Institutions and Customer Data: Complying with the Safeguards Rule, *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm.

[16] *See* Information Compromise and the Risk of Identity Theft: Guidance for Your Business, *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/idtrespond.pdf.

Service, the FTC has thus far conducted 19 seminars involving more than 2,780 officers from over 980 different agencies. This spring, the FTC and our training partners will conduct three such training sessions across California. The FTC staff also developed an identity theft case referral program, which examines patterns of identity theft activity in the Clearinghouse and then makes referrals to identity theft task forces around the country. Overall, the Clearinghouse is one of our best examples of how we can work together to combat identity theft.

## IV. The Role of Consumers

The undisputed MVP on the ID theft prevention team is the educated consumer. Education empowers, and nowhere is it more important than in the fight against identity theft.

As many of you may know, the Commission hosts a toll-free hotline, 1-877-ID THEFT, and a secure online complaint form on its website, www.consumer.gov/idtheft. We receive over 15,000 contacts per week from victims and consumers who want to avoid becoming a victim. Callers to the hotline receive counseling from trained personnel (including Spanish-speaking personnel) who, for example, advise victims to obtain their credit reports, request a fraud alert, contact creditors, and file a police report. The FTC's hotline is not the only place consumers can find counseling, however. Here in California, for example, the Identity Theft Resource Center and the Privacy Rights Clearinghouse have implemented stellar victim assistance programs.

The Commission also has developed and distributed step-by-step guides on how to avoid identity theft and how to deal with its effects.[17] These, and other materials, can be found on

---

[17] *See* ID Theft: What It's All About, *available at* http://www.ftc.gov/bcp/conline/pubs/credit/idtheftmini.pdf and Take Charge: Fighting Back Against Identity Theft *available at* http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm. Since February 2002, the FTC has distributed more than 1.9 million copies of the *Take Charge* booklet and recorded more than 2.3 million hits to the Web version.

the FTC's dedicated identity theft website.

We also have launched a number of efforts to simplify the victim recovery process. FTC staff worked with industry and consumer groups to develop an ID Theft Affidavit, a standard form for victims to use in resolving identity theft debts. This Affidavit has saved time for victims who previously often had to fill out multiple fraud affidavits. Now, our staff is working with the International Association of Chiefs of Police and industry and consumer groups on developing a universal police report for identity theft. Police reports are key to victim recovery because they show that identity theft has occurred and can serve as an "identity theft report" for the purpose of exercising certain new rights under the FACT Act.[18] They can, however, put an enormous strain on police department resources. The universal identity theft report would allow victims to complete a report at the Commission's website and take it to their local police department, where a police officer could verify the report through a victim interview and then provide confirmation to the FTC. It should simplify the recovery process for victims, lessen the burden on police departments, and provide assurances to companies that the information in the report is reliable.

Recent surveys demonstrate both progress and challenges in educating consumers. For example, the Visa International survey found that 63% of consumers say they are now more careful when disposing of financial statements and 62% say that they have become more discriminating about the sites at which they make purchases.[19] On the other hand, a recent survey conducted by the National Cyber Security Alliance found that over half of the respondents either had no anti-virus

---

[18] These include the right to an extended, seven-year fraud alert, the right to block fraudulent trade lines on credit reports, and the ability to obtain copies of fraudulent applications and transaction reports. *See* 15 U.S.C. § 1681 *et seq.*, as amended.

[19] *See supra* note 11.

protection or had not updated it within the past week, about half did not have a firewall, and 40% had no spyware protection. Yet, 83% said they were "safe from online threats." Of the respondents who had received a phishing email, 70% of those thought the phishing emails were from a legitimate company.[20]

These results tell me that government at all levels needs to re-double our efforts at educating consumers on how to protect their personal information. We continuously must work together to develop new, creative ways to get our messages out. Last fall, the FTC, together with partners from law enforcement, the technology industry, and nonprofits, launched OnGuard Online, an interactive, multi-media resource for information and up-to-the minute tools on how to recognize Internet fraud, avoid hackers and viruses, shop securely online, and deal with identity theft, spam, phishing, and file-sharing.[21]

And this spring, the FTC will launch a substantial new identity theft campaign to show consumers how to minimize their risk of falling victim to identity theft. The campaign will encourage consumers to "Deter, Detect, and Defend" against identity theft by taking steps to reduce their risk, keep a close eye on their personal information, and move quickly to minimize the damage if identity theft occurs. The centerpiece of the campaign is a turnkey toolkit – a comprehensive how-to guide on providing consumer education about identity theft. The toolkit, which includes everything from PowerPoint presentations to pamphlets, will empower consumers to educate each other on identity protection.

---

[20] *See* "AOL/NCSA Online Safety Study" (Dec. 2005), *available at* http://www.staysafeonline.info/pdf/safety_study_2005.pdf.

[21] *See* www.onguardonline.gov.

We recognize that, in developing all of these programs, it is important to have a clear understanding of the nature, extent, and prevalence of our adversary – identity theft. Although consumer complaints provide some information about these issues, the Commission has given a priority to collecting supplemental evidence through consumer surveys. We currently are conducting a new national identity theft survey, which should reveal any changes and new trends since our first survey in 2003.[22]

## V.Conclusion

Unlike professional football, identity theft does not have an off season. Together, we must combat identity theft 365 days per year. I understand that the heavy-lifting on this front is being done by state and local law enforcement. That being said, there are a number of ways that we can partner as we move forward. First, I encourage every organization, whether a government agency, consumer group, university, or business to share the ID theft prevention tips at OnGuardOnline.gov with employees, customers, students, members, and constituents. OnGuard Online is branded independently of the FTC, so that your organizations can make the website and the important information your own. Second, I encourage each of you to file comments and participate in the FTC's ongoing FACT Act rulemakings. Third, I hope that all of the law enforcement agencies participating in today's summit also will join the FTC at the three upcoming identity theft seminars to be held here in California this spring. And finally, I hope that every law enforcement agent will take advantage of the Identity Theft Data Clearinghouse, an invaluable resource. You can get more information about obtaining free access to the

[22] *See Federal Trade Commission – Identity Theft Survey Report* (Sept. 2003), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf.

Clearinghouse and the upcoming seminars at the FTC's booth located in the Summit exhibitor room.

I thank Governor Schwarzenegger and his Office of Privacy Protection for organizing this important summit, and the California District Attorneys association for hosting it. Thank you.