[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.*

One of the FTC's most recent la$iorsorcement actions arose from ChoicePoint's high-profile breach that occurred last year and was reported pursuant to Calisornia la$. 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 insormation 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 injun broke8al urc4.1(i)-1.1(cantsf.25 0 TD5 0Osi

[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).

[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

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 infion for losses rinformch a

[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

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

---

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

[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]

---

[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.