PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

Before the

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
SUBCOMMITTEE ON CONSUMER AFFAIRS,
PRODUCT SAFETY, AND INSURANCE
U.S. SENATE

on

Protecting Consumers' Phone Records

February 8, 2006

[2] For example, the Commission recently launched OnGuard Online, a campaign to educate consumers about the importance of safe computing. *See* www.onguardonline.gov. One module offers advice on avoiding spyware and removing it from computers. Another module focuses on how to guard against "phishing," a scam where fraudsters send spam or pop-up messages to extract personal and financial information from unsuspecting victims. Yet another module provides practical tips on how to avoid becoming a victim of identity theft. These

ese

[6] An act or practice is unfair if it: (1) causes or is likely to cause consumers substantial injury; (2) the injury is not reasonably avoidable by consumers; and (3) the injury is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

[7] *Id.* §§ 6801-09.

[8] *Id.* § 6821.

[9] *See* FTC press release "As Part of Operation Detect Pretext, FTC Sues to Halt Pretexting" (Apr. 18, 2001), *available at* http://www.ftc.gov/opa/2001/04/pretext.htm. For more information about the cases the Commission has brought under Section 521 of the GL

firms offering to conduct searches for consumers' financial data. The staff found approximately 200 firms that offered to obtain and sell consumers' asset or bank account information to third parties. The staff then sent notices to these firms advising them that their practices were subject to the FTC Act and the GLBA, and provided information about how to comply with the law.[10]

In conjunction with the warning letters, the Commission released a consumer alert, *Pretexting: Your Personal Information Revealed*, describing how pretexters operate and advising consumers on how to avoid having their information obtained through pretexting.[11] The alert warns consumers not to provide personal information in response to telephone calls, email, or postal mail, and advises them to review their financial statements carefully, to make certain that their statements arrive on schedule, and to add passwords to financial accounts.

While consumer education is important, it is only part of the FTC's efforts to combat pretexting. Aggressive law enforcement is critical. The FTC therefore followed up the first phase of *Operation Detect Pretext* in 2001 with a trio of law enforcement actions against information brokers.[12] In each of these cases, the defendants advertised that they could obtain non-public, confidential financial information, including information on checking and savings account numbers and balances, stock, bond, and mutual fund accounts, and safe deposit box

---

[10] *See* FTC press release "FTC Kicks Off Operation Detect Pretext" (Jan. 31, 2001), *available at* http://www.ftc.gov/opa/2001/01/pretexting.htm.

[11] *See* http://www.ftc.gov/bcp/conline/pubs/credit/pretext.htm.

[12] *FTC v. Victor L. Guzzetta, d/b/a Smart Data Systems*, No. CV-01-2335 (E.D.N.Y.) (final judgment entered Feb. 25, 2002); *FTC v. Information Search, Inc., and David Kacala*, No. AMD-01-1121 (D. Md.) (final judgment entered Mar. 15, 2002); *FTC v. Paula L. Garrett, d/b/a Discreet Data Systems*, No. H 01-1255 (S.D. Tex.) (final judgment entered Mar. 25, 2002).

unreasonably exposing consumer data to theft and misuse.[16] Companies that have failed to implement reasonable security and safeguard processes for consumer data face liability under various statutes enforced by the FTC, including the Fair Credit Reporting Act, the Safeguards provisions of the GLBA, and Section 5 of the FTC Act.[17]

In fact, two weeks ago the Commission announced a record-breaking proposed settlement with data broker ChoicePoint, Inc. This proposed settlement requires ChoicePoint to pay $10 million in civil penalties and $5 million in consumer redress to settle charges that its security and record-handling procedures violated the Fair Credit Reporting Act and the FTC Act. In addition, the proposed settlement requires ChoicePoint to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes, to establish and maintain a comprehensive information security program, and to obtain audits by an independent third-party security professional every other year until 2026. Further, the proposed settlement sends a strong signal to industry that it must maintain reasonable procedures for safeguarding

---

[16] In addition to law enforcement in the data security area, the Commission has provided business education about the requirements of existing laws and the importance of good security. *See, e.g.*, Safeguarding Customers' Personal Information: A Requirement for Financial Institutions, *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/safealrt.htm.

[17] *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); *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); *Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005). As the Commission has stated, an actual breach of security is not a prerequisite for enforcement under Section 5; however, evidence of such a breach may indicate that the company's existing policies and procedures were not adequate. It is important to note, however, that there is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution. *See* Statement of the Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on Data Breaches and Identity Theft (June 16, 2005) at 6, *available at* http://www.ftc.gov/os/2005/06/050616databreaches.pdf.

[18] News stories state that reporters obtained cell phone records of General Wesley Clark and cell phone and land line records of Canada's Privacy Commissioner Jennifer Stoddart. *See, e.g.,* Aamer Madhani and Liam Ford, *Brokers of Phone Records Targeted,* Chicago Trib., Jan. 21, 2006, *available at* 2006 WLNR 1167949.

[19] Albeit anecdotal, news articles illustrate some harmful uses of telephone records. For example, data broker Touch Tone Information Inc. reportedly sold home phone numbers and addresses of Los Angeles Police Department detectives to suspected mobsters, who then used the information in an apparent attempt to intimidate the police officers and their families. *See, e.g.,* Peter Svensson, *Calling Records Sales Face New Scrutiny,* Wash. Post, Jan. 18, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/01/18/AR200601180165 9.html.

[20] Under Section 13(b) of the FTC Act, the Commission has the authority to file actions in federal district court against those engaged in deceptive or unfair practice

[21] Consumer telephone records are considered "customer proprietary network information" under the Telecommunications Act of 1996 ("Telecommunications Act"), which amended the Communications Act, and accordingly are afforded privacy protections by the regulations under that Act. *See* 42 U.S.C. § 222; 47 C.F.R. §§ 64.2001- 64.2009. The Telecommunications Act requires telecommunications carriers to secure the data, but does not specifically address pretexting to obtain telephone records. Moreover, the FTC's governing statute specifically states that the Commission lacks jurisdiction over common carrier activities that are subject to the Communications Act. 15 U.S.C. § 46(a). The Commission opposed this jurisdictional gap during the two most recent reauthorization hearings. *See* http://www.ftc.gov/os/2003/06/030611reauthhr.htm; *see also* http://www.ftc.gov/os/203/06/030611learysenate.htm; http://www.ftc.gov/os/2002/07/sfareauthtest.htm

IV. Conclusion

Protecting the privacy of consumers' data requires a multi-faceted approach: coordinated law enfo