

PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

Before the

COMMITTEE ON ENERGY AND COMMERCE
U.S. HOUSE OF REPRESENTATIVES

on

Phone Records for Sale:
Why Aren't Phone Records Safe From Pretexting?

February 1, 2006

I. Introduction

Mr. Chairman, Mr. Dingell, and members of the Committee, I am Jon Leibowitz, Commissioner of the Federal Trade Commission (“FTC” or “Commission”).¹ I appreciate the opportunity to discuss telephone records pretexting and the Commission’s significant work to protect the privacy and security of telephone records and other types of sensitive consumer information. The Commission is currently investigating companies that offer consumer telephone records for sale, and we plan to pursue these investigations vigorously.

Maintaining the privacy and security of consumers’ personal information is one of the Commission’s highest priorities. Companies that engage in pretexting – the practice of obtaining personal information, such as telephone records, under false pretenses – not only violate the law, but they undermine consumers’ confidence in the marketplace and in the security of their sensitive data. While pretexting to acquire telephone records has recently become more prevalent, the practice of pretexting is not new. The Commission has used its full arsenal of tools to attack scammers who use fraud to gain access to consumers’ personal information.

Aggressive law enforcement is at the center of the FTC’s efforts to protect consumers’ sensitive information. The Commission has taken law enforcement action against companies allegedly offering surreptitious access to consumers’ financial records, and will continue to challenge business practices that unnecessarily expose consumers’ sensitive information. The Commission also continues to provide consumer education and outreach to industry to ensure

¹ The views expressed in this statement represent the views of the Commission. My oral testimony and responses to questions reflect my own views and do not necessarily represent the views of the Commission or any individual Commissioner.

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

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 GLBA, see http://www.ftc.gov/privacy/privacyinitiatives/pretexting_enf

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/online/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, last week 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 sensitive

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/online/pubs/alerts/safealrt.htm>.

¹⁷ *United States v. ChoicePoint, Inc.* (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>.

consumer information and protecting it from data thieves.

III. Pretexting for Consumers' Telephone Records

An entire industry of companies offering to provide purchasers with the cellular and land line phone records of third parties recently has developed. Recent press stories report on the successful purchase of the phone records of prominent figures.¹⁸ Although the acquisition of telephone records does not present the opportunity for immediate financial harm as the acquisition of financial records does, it nonetheless is a serious intrusion into consumers' privacy and could result in stalking, harassment, and embarrassment.¹⁹ Although pretexting for consumer telephone records is not prohibited by the GLBA, the Commission may bring a law enforcement action against a pretexter of telephone records for deceptive or unfair practices under Section 5 of the FTC Act.²⁰

The Commission is currently investigating companies that appear to be engaging in

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.,* Amer 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/AR2006011801659.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 practices and obtain injunctive relief and other equitable relief, including monetary relief in the form of consumer redress or disgorgement of ill-gotten profits. However, the FTC Act does not authorize the imposition of civil penalties for an initial violation, unless there is a basis for such penalties, i.e., an applicable statute, rule or litigated decree.

telephone pretexting. Using the approach that proved successful in *Operation Detect Pretext*, Commission staff surfed the Internet for companies that offer to sell consumers' phone records.

FTC staff then identified appropriate targets for investigation and completed undercover

purchases of phone records. Commission home 0.0000 cm0.00 0.000000 0.0000 0.0000 cm0.00 0.00 0.00 rg

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>.

²² In addition, the Attorneys General of Florida, Illinois, and Missouri recently sued companies allegedly engaged in pretexting. *See* http://myfloridalegal.com/_852562220065EE67.nsf/0/D510D79C5EDFB4B98525710000Open&Highlight=0,telephone,records; http://www.ag.state.il.us/pressroom/2006_01/20060120.html; <http://www.ago.mo.gov/newsreleases/2006/012006b.html>. Several telecommunications carriers also have sued companies that reportedly sell consumers' phone records. According to press reports, Cingular Wireless, Sprint Nextel, T-Mobile, and Verizon Wireless have sued such companies. *See, e.g.,* <http://www.upi.com/Hi-Tech/view.php?StoryID=20060124-011904-6403r>; <http://www.wired.com/news/technology/1,70027-0.html>; http://news.zdnet.com/2100-1035_22-6031204.html.

IV. Conclusion

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