PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

Before the

COMMITTEE ON ENERGY AND COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

on

"Combating Pretexting: H.R. 936, Prevention of Fraudulent Access to Phone Records Act"

March 9, 2007

I. Introduction

Chairman Dingell, Ranking Member Barton, and members of the Committee, I am Lydia Parnes, Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to discuss the practice of obtaining unauthorized access to consumers' sensitive information through fraud, a practice known as "pretexting," as well as the Commission's significant work to protect the privacy and security of telephone records and other types of sensitive consumer information. I also appreciate the opportunity to comment on the proposed Prevention of Fraudulent Access to Phone Records Act, H.R. 936. The Committee's work in this area has been important in protecting consumers.

Ensuring the privacy and security of consumers' personal information is one of the Commission's highest priorities. Individuals or companies that procure through pretexting or sell on the open market confidential consumer information without the consumer's knowledge or consent not only violate the law, but they undermine consumers' confidence in the marketplace and in the security of their sensitive data. Accordingly, the Commission has used its full arsenal of tools to attack the pretexters and the brokers who sell pretexted information. Since 2006, the Commission initiated a half dozen law enforcement actions against online data brokers and pretexters of confidential consumer telephone records. The Commission also has developed and disseminated a variety of new online and written materials to educate consumers about protecting their sensitive personal information in general and from pretexting in particular.

Today, I will first discuss the FTC's efforts to protect consumers from the sale of phone

---

[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.

records obtained through pretexting. Next, I will provide a brief history of the FTC's enforcement efforts in the area of pretexting for financial information. I will then address the provisions of H.R. 936.

II. FTC Enforcement Efforts Against Firms Selling Telephone Records

Aggressive law enforcement is at the center of the FTC's efforts to protect consumers' telephone call records from pretexting. The acquisition of such records by unauthorized third parties is a serious intrusion into consumers' privacy that presents a significant risk of harm. Evidence obtained in the Commission's law enforcement actions reveals truly horrifying incidents of stalking and harassment of consumers whose call records were pretexted.[2]

Last May, the Commission announced an initial wave of five lawsuits in federal courts across the country against online data brokers, alleging that the defendants had engaged in unfair practices, prohibited by Section 5 of the FTC Act,[3] when they obtained and sold consumer

---

[2] Several consumers whose phone records were obtained and sold by the defendants in one of the FTC's pending phone pretexting cases have submitted signed declarations, attesting that they have been stalked and physically threatened by, for example, a former co-worker, an ex-spouse. and an ex-boyfriend. In addition to the real threat posed to their safety, these consumers have spent significant time and hundreds of dollars changing phone numbers or service providers. *See Br. of Pl. FTC in Supp. of Mot. for Summ. J.* at 8-14, *FTC v. AccuSearch, Inc.*, No. 06-CV-0105 (D. Wyo. Jan. 22, 2007).

In addition, there have been media reports of other incidents of pretexting that led to harm. One data broker 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 detectives and their families. *See, e.g.*, Peter Svensson, *Calling Records Sales Face New Scrutiny,* Wash. Post, Jan. 18, 2006, *available at* www.washingtonpost.com/wp-dyn/content/ article/2006/01/18/AR2006011801659.html.

[3] 15 U.S.C. § 45(a). 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. *Id.* at § 45(n). Under Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), the Commission has the authority to file actions in federal district court to obtain injunctions and other equitable relief against those

telephone records without the consumer's knowledge or authorization.[4] In each of these cases, the defendant advertised on its website that it could obtain confidential customer phone records from telecommunications carriers for fees ranging from $65 to $180. The complaints alleged that the defendants, or persons they hired, obtained this information by using false pretenses, including posing as the carrier's customer, to induce the carrier's employees to disclose the records.

To date, the Commission has settled two of these cases, obtaining permanent injunctions that bar the defendants from selling customer phone records or consumer personal information derived from such records.[5] In addition, the settlements require the defendants to disgorge the profits they derived from the alleged illegal operations.[6] The remaining three cases are still in active litigation.

The FTC's first wave of phone pretexting cases was the culmination of extensive investigations of this industry. Commission staff surfed the Internet for companies that offered to sell consumers' phone records, then identified appropriate targets for investigation and

---

engaged in violations of Section 5.

[4] *FTC v. Info. Search, Inc.*, No. 1:06-CV-01099-AMD (D. Md. filed May 1, 2006); *FTC v. AccuSearch, Inc.*, No. 06-CV-0105 (D. Wyo. filed May 1, 2006); *FTC v. CEO Group, Inc.*, No. 06-60602 (S.D. Fla. filed May 1, 2006); *FTC v. 77 Investigations, Inc.*, No. EDCV06-0439 VAP (C.D. Cal. filed May 1, 2006); *FTC v. Integrity Sec. and Investigation Servs., Inc.*, No. 2:06-CV-241-RGD-JEB (E.D. Va. filed May 1, 2006).

[5] *FTC v. Integrity Sec. and Investigation Servs., Inc., supra* note 4 (final judgment entered Oct. 30, 2006) *available at* www.ftc.gov/os/caselist/pretextingsweep/061005isisstipfinalord.pdf; and *FTC v. Info. Search, Inc., supra* note 4 (final judgment entered Feb. 22, 2007).

[6] The FTC does not have authority to obtain civil penalties in these cases, and therefore is limited to the equitable remedy of disgorgement. As currently drafted, H.R. 936 would authorize the Commission to seek civil penalties.

completed undercover purchases of the records. For some of these companies, staff sent warning letters and followed up later to ensure that they were no longer selling consumer phone records. Other companies became targets for enforcement action, as described above.

The Commission has been assisted greatly in its efforts by the Federal Communications Commission, which has jurisdiction over telecommunications carriers subject to the Telecommunications Act.[7] Our two agencies are committed to coordinating our work on this issue, as we have done successfully in enforcing the "National Do Not Call" implementation legislation.

Building upon evidence gathered in its initial cases, last month the Commission filed a sixth case in federal district court in Florida against several defendants that allegedly conducted or directed the actual pretexting and obtained consumers' phone records on behalf of others.[8]

---

[7] 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. The FTC's governing statute exempts from Commission jurisdiction common carrier activities that are subject to the Communications Act. 15 U.S.C. § 46(a). The Commission recommended that Congress remove this exemption at its two most recent reauthorization hearings and in testimony on FTC jurisdiction over broadband Internet access service before the Senate Judiciary Committee in June 2006. *See* http://www.ftc.gov/os/2003/06/030611reauthhr.htm; http://www.ftc.gov/os/2003/06/030611reauthsenate.htm; *see also* http://www.ftc.gov/os/203/06/030611learysenate.htm; http://www.ftc.gov/os/2002/07/sfareauthtest.htm; http://www.ftc.gov/os/2006/06/p052103CommissionTestimonyReBroadbandInternetAcess Services06142006Senate.pdf.

[8] *FTC v. Action Research Group, Inc.*, No. 6:07-cv-227-Orl-22JGG, (M.D. Fla. filed Feb. 14, 2007). Several of the defendants named in the FTC's complaint are also the subject of federal and state criminal actions in California, stemming from the well-publicized phone records pretexting of Hewlett-Packard board members and journalists. *See, e.g.,* Matt Richtel, *With a Little Stealth, Just About Anyone Can Get Phone Records,* NY Times, Sep. 7,

The FTC alleged that Action Research Group and its principals and agents obtained and sold consumers' confidential phone records without their knowledge or consent. This case connects the phone records pretexters to the middlemen who sell the records to third parties. In addition to alleging that the unauthorized sale of phone records is an unfair practice, the FTC's complaint alleges that the defendants engaged in deceptive practices by obtaining the records through the use of fraud and misrepresentations. The agency has asked the court to stop the conduct and to order the defendants to give up their ill-gotten gains.

III. FTC's History of Combating Financial Pretexting

In addition to the recent cases involving telephone records pretexting, the Commission has brought actions under Section 5 of the FTC Act and Section 521 of the Gramm-Leach-Bliley Act ("GLBA") against businesses and individuals who used false pretenses to obtain and sell financial information without consumer consent.

The Commission filed its first pretexting case against a company that offered to provide consumers' financial records to anybody for a fee.[9] According to the complaint, the company's employees allegedly obtained these records from financial institutions by posing as the consumer whose records were being sought. The complaint charged that this practice was both deceptive and unfair under Section 5 of the FTC Act.

In 1999, Congress passed the GLBA, which provided another tool to attack the

---

2006, *available at* http://www.nytimes.com/2006/09/07/technology/07phone.html?ex=1158465600&en=2f20498c7fcc7e5b&ei=5070.

[9] *FTC v. James J. Rapp*, No. 99WM-783 (D. Colo. final judgment entered June 22, 2000), *available at* http://www.ftc.gov/os/2000/06/touchtoneorder.

unauthorized acquisition of consumers' financial information.[10] Section 521 of the GLBA prohibits "false, fictitious, or fraudulent statement[s] or representation[s] to an officer, employee, or agent of a financial institution" to obtain customer information from a financial institution.[11]

To ensure awareness of and compliance with the then-new anti-pretexting provisions of the GLBA, the Commission launched Operation Detect Pretext in 2001.[12] Operation Detect Pretext combined a broad monitoring program, the widespread dissemination of industry warning notices, consumer education, and aggressive law enforcement.

In the initial monitoring phase of Operation Detect Pretext, FTC staff conducted a "surf" of more than 1,000 websites and a review of more than 500 advertisements in print media to identify 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 providing information about how to comply with the law.[13]

The Commission followed its education campaign with aggressive law enforcement,

---

[10] 15 U.S.C. §§ 6821-6827

[11] *Id.* at § 6821.

[12] 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.

[13] FTC press release, "FTC Kicks Off Operation Detect Pretext" (Jan. 31, 2001), *available at* http://www.ftc.gov/opa/2001/01/pretexting.htm. 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, *available at* http://www.ftc.gov/bcp/conline/pubs/credit/pretext.htm.

including a trio of law enforcement actions filed in 2001 against information brokers.[14] 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 locations, for fees ranging from $100 to $600. Based on evidence obtained in undercover investigations, the FTC alleged that the defendants or persons they hired called banks and posed as customers to obtain balances on checking accounts. The defendants in each of the cases ultimately agreed to settlements that barred them from further violations of the law and required them to surrender ill-gotten gains.[15] Since GLBA's passage, the FTC has brought over a dozen cases alleging violations of Section 521 in various contexts.[16]

Because the anti-pretexting provisions of the GLBA provide for criminal penalties, the Commission also may refer financial pretexters to the U.S. Department of Justice for criminal prosecution, as appropriate. Following one such referral, an individual pled guilty to one count of pretexting under the GLBA.[17]

IV. FTC Education and Outreach

---

[14] *FTC v. Victor L. Guzzetta*, No. CV-01-2335 (E.D.N.Y. final judgment entered Feb. 25, 2002); *FTC v. Info. Search, Inc.*, No. AMD-01-1121 (D. Md. final judgment entered Mar. 15, 2002); *FTC v. Paula L. Garrett,* No. H 01-1255 (S.D. Tex. final judgment entered Mar. 25, 2002).

[15] *See* www.ftc.gov/opa/2002/03/pretextingsettlements.htm.

[16] *See* www.ftc.gov/privacy/privacyintiatives/pretexting_enf.htm.

[17] *United States v. Peter Easton*, No. 05 CR 0797 (S.D.N.Y. final judgment entered Nov. 17, 2005).

In addition to its law enforcement efforts, the Commission has an extensive program to teach consumers and businesses better ways to protect sensitive data. For example, in February 2006, 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.

The FTC also recently launched a nationwide identity theft education program, "Avoid ID Theft: Deter, Detect, Defend," which broadly advises consumers on how to avoid becoming victims of identity theft. The message for consumers is that they can (1) deter identity thieves by safeguarding their personal information; (2) detect suspicious activity by routinely monitoring their financial accounts, billing statements, and credit reports; and (3) defend against ID theft as soon as they suspect it. The Deter, Detect, Defend campaign has been very popular. The FTC has distributed more than 1.5 million brochures to consumers and 30,000 kits to employers, community groups, members of Congress, and others to educate their constituencies. The kits contain a victim recovery guide, a training booklet, a guide to talking about identity theft, presentation slides, an easy-to-read brochure, and a 10-minute video that organizations can use to educate their employees, customers, and communities about identity theft.

The FTC also sponsors an innovative multimedia website, OnGuardOnline, designed to educate consumers about basic computer security.[18] The website provides information on specific topics such as phishing, spyware, and identity theft. Since its launch in late 2005, OnGuardOnline has attracted more than 3.5 million visits. All of these materials are part of the

---

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

Commission's comprehensive library on consumer privacy, data security, and identity theft.[19]

V. The Prevention of Fraudulent Access to Phone Records Act, H.R. 936

As described above, the Commission has used its jurisdiction under Section 5 of the FTC Act to take action against individuals and business engaged in the pretexting or sale of confidential phone records obtained through pretexting. Although Section 5 is a powerful tool, the Commission continues to support the enactment of more specific prohibitions against phone pretexting that provide additional remedies for violations.[20]

The proposed Prevention of Fraudulent Access to Phone Records Act (the "Phone Records Act") contains several important components that would assist the Commission in combating phone pretexting. First, in addition to prohibiting pretexting itself, the Phone Records Act would extend liability to individuals who solicit such records and knew or should have known that the records would be obtained through false pretenses. The Commission agrees that those who solicit pretexting should be held responsible, and that the knowledge standard contained in the Phone Records Act is the appropriate one, because it would prevent data brokers from turning a "blind eye" to the manner in which their sources obtain phone records.

The Phone Records Act also would allow the FTC to recover civil penalties from violators. Often, monetary penalties can be the most effective civil remedy in privacy-related actions and, as noted earlier, the Commission currently is unable to obtain this remedy in phone pretexting cases brought under the FTC Act. Finally, the Phone Records Act contains an important exemption for law enforcement agencies in connection with their official duties.

---

19 *See* www.ftc.gov/privacy/index.html.

20 *See* Commission Testimony from the 109th Congress before this Committee, *available at* http://www.ftc.gov/opa/2006/09/houseenergy.htm.

In addition to the Phone Records Act, two recently passed statutes will assist in the fight against phone pretexting. First, in December 2006, Congress passed and the President signed the "US SAFE WEB Act" into law.[21] This Act allows greater cooperation and information sharing between law enforcers in the United States and their counterparts in other countries. In developing the Commission's phone pretexting cases, FTC staff learned that some websites offering consumer telephone records were registered to foreign addresses. The US SAFE WEB Act will assist the Commission in pursuing data brokers who are operating outside the United States.

Second, Congress recently approved and, on January 12, 2007, President Bush signed into law the Telephone Records and Privacy Protection Act,[22] which criminalizes obtaining confidential records by making false statements to a telephone service provider. The Commission anticipates that its ongoing actions against phone records pretexting will lead to criminal law enforcement referrals to our sister agency, the Department of Justice.

VI. Conclusion

Protecting the privacy of consumers' telephone records requires a multi-faceted approach: coordinated law enforcement by government agencies against the pretexters; efforts by the telephone carriers to protect their records from intrusion; and outreach to educate consumers on actions they can take to protect themselves. The Commission has been at the forefront of efforts to safeguard consumer information and is committed to continuing its work in this area. The Commission looks forward to continuing to work with this Committee to protect the privacy and

---

[21] The Undertaking Spam, Spyware, and Fraudulent Enforcement with Enforcers Across Borders Act of 2006, Pub. L. No. 109-455, 120 Stat. 3372.

[22] Telephone Records and Privacy Protection Act, Pub. L. No: 109-476.

security of sensitive consumer information.