PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

Before the

COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
U.S. HOUSE OF REPRESENTATIVES

on

Internet Data Brokers and Pretexting: Who Has Access to Your Private Records?

September 29, 2006

I. Introduction

Chairman Whitfield, Ranking Member Stupak, and members of the Subcommittee, I am Joel Winston, Associate Director of the Division of Privacy and Identity Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to discuss how data brokers obtain unauthorized access to consumer telephone records through deceit, a practice known as "pretexting," and the Commission's significant work to protect the privacy and security of telephone records and other types of sensitive consumer information. In testimony before the full Committee on Energy and Commerce in February 2006, the Commission reported that it was actively investigating companies that obtained and sold consumer telephone records.[2] Subsequently, in May 2006, the Commission filed five lawsuits in federal courts across the country against online data brokers that, directly or through third parties, allegedly obtained and sold consumer telephone records without the consumer's knowledge or consent.[3] Today the Commission announced a settlement in one of these cases,[4] while the remaining cases are

---

[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] "Phone Records for Sale: Why Aren't Phone Records Safe from Pretexting?" 109th Cong. (Feb. 1, 2006) (written statement of the Federal Trade Commission at 1, 7-8) *available at* http://energycommerce.house.gov/108/Hearings/02012006hearing1763/Leibowitz.pdf.

[3] *FTC v. Info. Search, Inc.*, No. 1:06-CV-01099-AMD (D. Md. filed May 1, 2006); *FTC v. AccuSearch, Inc. d/b/a Abika.com*, No. 06-CV-0105 (D. Wyo. filed May 1, 2006); *FTC v. CEO Group, Inc. d/b/a Check Em Out*, 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. & Investigation Servs., Inc.*, No. 2:06-CV-241-RGD-JEB (E.D. Va. filed May 1, 2006).

[4] Pursuant to the settlement terms that are subject to court approval, defendant Integrity Security and Investigation, Services, Inc. ("ISIS") and its principal, Edmund Edmister,

pending. Further, during the pendency of these matters, the Commission continues to investigate vigorously other firms and individuals that may be engaged in telephone records pretexting.

Protecting the privacy and security of consumers' personal information is one of the Commission's highest priorities. Companies that engage in pretexting not only violate the law, they also undermine consumers' confidence in the marketplace and in the security of their sensitive data. While pretexting to acquire telephone records has gained attention recently,[5] the practice of pretexting is not new. Over the years, 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. In addition to the Commission's recent lawsuits against data brokers who sold consumer telephone records, the FTC has taken law enforcement action against several companies allegedly offering surreptitious access to consumers' financial records as well as against companies that allegedly failed to implement reasonable procedures for safeguarding consumers' sensitive data. Such efforts demonstrate the Commission's commitment to challenging business practices that unnecessarily expose consumers' sensitive data and to helping

---

have agreed to be permanently enjoined from obtaining, causing others to obtain, marketing, or selling customer phone records or consumer personal information that is derived from such records. In addition, the settlement requires ISIS and Edmister to disgorge any ill-gotten gains derived from the alleged violations.

[5] This practice recently returned to the public spotlight with reports that Hewlett-Packard Co. ("HP") officials had hired a security consultant that used another firm to obtain the call records of HP board members and journalists. *See, e.g.*, Matt Richtel, *With a Little Stealth, Just About Anyone Can Get Phone Records*, N.Y. Times, Sept. 7, 2006, *available at* http://www.nytimes.com/2006/09/07/technology/07phone.html?ex=1158465600&en=2f20498c7fcc7e5b&ei=5070.

consumers protect themselves against criminals who would steal their personal information.[6]

Today I will first discuss the FTC's recent efforts to protect consumers from individuals and firms engaged in pretexting for telephone records. Second, I will provide a brief history of the FTC's enforcement efforts in the related area of pretexting for financial information. Finally, I will conclude with several recommendations for legislative action that would assist the Commission's efforts to curtail pretexting for telephone records. As explained more fully below, the Commission urges Congress to enact specific prohibitions against telephone records pretexting and to allow the Commission to seek civil penalties against violators of such legislation.

II. FTC Enforcement Efforts Against Firms Selling Telephone Records

On May 1, 2006, the Commission filed lawsuits against five companies and their principals alleging that they sold confidential consumer call records obtained through fraud or other illegal means. The complaints charge the defendants with violating Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[7] In each of these cases, the defendants advertised on their websites that they could obtain confidential

---

[6] The Commission also has an extensive program to teach consumers and businesses better ways to protect sensitive data. For example, in September 2005, the Commission 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 materials are additions to our comprehensive library on consumer privacy and security. *See* www.ftc.gov/privacy/index.html.

[7] 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.* § 45(n).

customer phone records from telecommunications carriers for fees ranging from $65 to $180. The FTC alleged that the defendants or persons they hired obtained this information by using false pretenses, including posing as the phone carrier's customer to induce the telephone company's employees to disclose the records. The complaints seek a permanent injunction to prohibit the future sale of phone records and request the courts to disgorge any profits obtained through the defendants' alleged illegal operations.[8]

These Commission actions are in response to the development of an industry of individuals and companies that offer to sell to the general public the cellular and land line phone records of third parties. Earlier this year, news articles reported on the successful purchase of the phone records of prominent figures.[9] Although the acquisition of telephone records does not present the same risk of 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.[10] And while there is no specific federal civil law that prohibits

---

[8] Under current law, the Commission does not have authority to seek civil penalties in these cases.

[9] According to these reports, reporters hired pretexters to obtain the cell phone call records of General Wesley Clark and the cell phone and land line call 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.

[10] Although 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.

pretexting for consumer telephone records,[11] 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.[12]

The Commission's lawsuits against the five data brokers were the culmination of investigations into companies that appeared to be engaging in telephone records pretexting. Commission staff surfed the Internet for companies that offered to sell consumers' phone records, then identified appropriate targets for investigation and completed undercover purchases of phone records.

The FTC gathered important data in support of these cases by working closely with the Federal Communications Commission, which has jurisdiction over telecommunications carriers subject to the Telecommunications Act.[13] Our two agencies are committed to coordinating our

---

[11] As discussed below, the Gramm-Leach-Bliley Act ("GLBA") prohibits pretexting to obtain or attempt to obtain customer information of a financial institution. 15 U.S.C. § 6821. In addition, the practice may violate some state laws that prohibit telephone records pretexting as well as various criminal statutes. *See, e.g.*, 18 U.S.C. § 1343.

[12] 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. 15 U.S.C. § 53(b).

[13] 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 recent 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;

work on this issue, as we have done successfully with the enforcement of the "National Do Not Call" legislation.[14]

In the course of the litigation, FTC staff have learned further details about the nature of the alleged practices. In many cases, it appears that the entity that advertises the sale of call records does not perform the actual pretexting, but contracts with another party to do so. As stated above, the Commission continues to investigate various firms and individuals that comprise this industry.

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 GLBA against businesses that use false pretenses to obtain financial information without consumer consent.

The Commission filed its first pretexting case against a company that offered to provide

---

http://www.ftc.gov/os/2003/06/030611reathsenate.htm; *see also* http://www.ftc.gov/os/2003/06/030611learysenate.htm; http://www.ftc.gov/os/2002/07/sfareauthtest.htm; http://www.ftc.gov/os/2006/06/P052103CommissionTestimonyReBroadbandInternetAccessServices06142006Senate.pdf.

[14] In addition, the Attorneys General of California, Texas, Florida, Illinois, and Missouri have sued companies allegedly engaged in pretexting. *See* news releases *available at* http://ag.ca.gov/newsalerts/release.php?id=1269;http://www.oag.state.tx.us/oagnews/release.php?id=1449; 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/news releases/2006/012006b.html. Several telecommunications carriers also have sued companies that reportedly sell consumers' phone records. According to press reports, AT&T, 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.

consumers' financial records to anybody for a fee.[15] According to the complaint, the company's employees allegedly obtained these records from financial institutions by posing as the consumer whose records it was seeking. The complaint charged that this practice was both deceptive and unfair under Section 5 of the FTC Act.[16]

In 1999, Congress passed the GLBA, which provided another tool to attack the unauthorized acquisition of consumers' financial information.[17] 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 of a financial institution.[18]

To ensure awareness of and compliance with the then-new anti-pretexting provisions of the GLBA, the Commission launched Operation Detect Pretext in 2001.[19] Operation Detect Pretext included 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

---

[15] *FTC v. James J. Rapp & Regana L. Rapp, d/b/a Touch Tone Info., Inc.*, No. 99-WM-783 (D. Colo.) (final judgment entered June 22, 2000), *available at* http://www.ftc.gov/os/2000/06/touchtoneorder.

[16] 15 U.S.C. § 45(a), (n).

[17] *Id.* §§ 6801-09.

[18] *Id.* § 6821.

[19] *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. Since GLBA's passage, the FTC has brought over a dozen cases alleging violations of Section 521 in various contexts.

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.[20]

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.[21] 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.

The Commission followed its consumer education campaign with aggressive law enforcement. The FTC followed up the first phase of *Operation Detect Pretext* in 2001 with a trio of law enforcement actions against information brokers.[22] 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. The

---

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

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

[22] *FTC v. Victor L. Guzzetta, d/b/a Smart Data Sys.*, 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, d/b/a Discreet Data Sys.*, No. H 01-1255 (S.D. Tex.) (final judgment entered Mar. 25, 2002).

FTC alleged that the defendants or persons they hired called banks, posing as customers, to obtain balances on checking accounts.[23]

The FTC's complaints alleged that the defendants' conduct violated the anti-pretexting prohibitions of the GLBA, and further was unfair and deceptive in violation of Section 5 of the FTC Act. 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.[24]

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.[25]

Finally, the Commission is aware that it is not enough to focus on the purveyors of illegally obtained consumer data. It is equally critical to ensure that entities that handle and maintain sensitive consumer information have in place reasonable and adequate processes to protect that data. Accordingly, in several recent cases, the Commission has challenged data

---

[23] In sting operations set up by the FTC in cooperation with banks, investigators established dummy bank account numbers in the names of cooperating witnesses and then called defendants, posing as purchasers of their pretexting services. In the three cases, an FTC investigator posed as a consumer seeking account balance information on her fiancé's checking account. The defendants or persons they hired proceeded to call the banks, posing as the purported fiancé, to obtain the balance on his checking account. The defendants later provided the account balances to the FTC investigator.

[24] *See* FTC press release "Information Brokers Settle FTC Charges" (Mar. 8, 2002), *available at* http://www.ftc.gov/opa/2002/03/pretextingsettlements.htm.

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

security practices as unreasonably exposing consumer data to theft and misuse.[26] 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.[27]

In one such recent case, the Commission announced a settlement with data broker ChoicePoint, Inc, requiring 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 settlement required 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. This settlement and the other Commission enforcement actions in this area send a strong signal that industry must maintain reasonable procedures for safeguarding sensitive

---

[26] 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.

[27] *See, e.g., In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006); *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 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 Comm. 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.

IV. Recommendations

The Commission has been effective in exercising its jurisdiction under Section 5 of the FTC Act in an effort to combat the use of pretexting by individuals and businesses to obtain sensitive consumer data. However, it would further assist the FTC's enforcement in this area to have more specific prohibitions against pretexting for consumer telephone records and soliciting or selling consumer telephone records obtained through actual or reasonably known pretexting activity. In addition, the Commission recommends that any such legislation contain appropriate exceptions for specified law enforcement purposes. Such a statutory framework would send a strong message to this industry: pretexting for consumer telephone records is clearly and unequivocally illegal.

The FTC also recommends that Congress as part of any such legislation give the Commission authority to seek civil penalties against violators, a remedy that the FTC does not currently have in cases involving telephone records pretexting. Often, penalties can be the most effective civil remedy in these areas to provide real deterrence.

Finally, FTC staff learned through its investigation that some websites offering consumer telephone records were registered to foreign addresses. This finding underscores the importance of the Commission's previous recommendation that Congress enact cross-border fraud legislation. The proposal, called the "US SAFE WEB Act," will overcome many of the existing obstacles to information sharing in cross-border investigations.[28]

---

[28] The Undertaking Spam, Spyware, and Fraudulent Enforcement with Enforcers Across Borders Act, S. 1608, 109th Congress (2006) (passed by the Senate on Mar. 16, 2006).

V. 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 self-protection actions they can take. 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 working with this Subcommittee to protect the privacy and security of sensitive consumer information.