PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

ALTERNATIVE HORMONE REPLACEMENT THERAPY PRODUCTS

Before the

SENATE SPECIAL COMMITTEE ON AGING

Washington, DC

April 19, 2007

I. Introduction

Chairman Kohl, Ranking Member Smith, and Members of the Committee, I am Eileen Harrington, Deputy Director of the Bureau of Consumer Protection of the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to discuss the Commission's efforts to address the misleading online advertising of "alternatives" to hormone replacement therapy as well as its work to combat all types of Internet fraud.

Among its many benefits, the Internet provides consumers with access to a vast array of information and products, including health-related items. Unfortunately, the online medium also provides an opportunity for irresponsible marketers to prey on consumers with false or misleading claims that can cause economic injury and have potentially serious consequences for consumers' health. Therefore, pursuant to its broad authority to prevent "unfair or deceptive acts or practices,"[2] the FTC has a longstanding and active program to protect consumers in the online environment.

This testimony provides an overview of the FTC's efforts with respect to health-related fraud, including an explanation of its jurisdiction over health products and a discussion of the FTC/FDA project to address the misleading marketing of hormone replacement therapy alternatives. Pursuant to the Committee's request, the testimony then discusses the FTC's broader program to combat online scams in general.

---

[1] This written statement presents the views of the Commission. My oral testimony and responses to questions reflect my views and do not necessarily represent the views of the Commission or any individual Commissioner.

[2] Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a). In addition, Section 12 of the Federal Trade Commission Act prohibits the false advertisement of "food, drugs, devices, services, and cosmetics." 15 U.S.C. § 52.

II. Health-Related Fraud

A. Overview

The Commission employs a three-pronged strategy to protect consumers from deceptive claims for health-related products: (1) law enforcement; (2) consumer education; and (3) business outreach. In each of these areas, the FTC works closely with its state, federal, and international partners, including state attorneys general, the Food and Drug Administration ("FDA"), and members of the Me

diet and fitness products.[5] For example, the FTC issued a Consumer Alert on HGH pills and sprays.[6] Most recently, the Commission released its "Glucobate" teaser website advertising a phony miracle product to help consumers avoid deceptive diabetes claims.[7]

On the business outreach front, the Commission has created numerous materials geared toward helping businesses avoid making deceptive claims. For instance, the FTC's publication "Dietary Supplements: An Advertising Guide for Industry," provides easy-to-understand explanations of advertising standards for the marketing of health products, along with many useful examples.[8]

On all three fronts, the FTC frequently collaborates with the FDA on health issues. Although the FTC and the FDA both have jurisdiction over health-related products, the agencies coordinate closely pBDC 6 49 0 0 apt Tc -0.0rsuant t.36 Tdoi30 pt f a long.36 Td2 the ageew74-2.3.36 Td2 38llab

unique to the computer age, such as pagejacking, phishing, and modem hijacking.[16] Since 1994, the FTC has filed 538 actions against individuals and corporations that have used the Internet to unleash a wide variety of deceptive and unfair practices on American consumers. The Commission's efforts to address deceptive spam and spyware illustrate this broader Internet fraud program and the tools the FTC employs to combat online scams.

Since 1997, the Commission has filed 89 actions against 241 defendants in which spam was an integral element of a scheme that harmed consumers.[17] Twenty-six of these cases were filed after Congress enacted the CAN-SPAM Act,[18] which, among other things, prohibits email senders from using deceptive message headers and subject lines. In many instances, scam artists use unsolicited commercial email to put a new twist on schemes that previously could be conducted in the offline world. For example, last year the FTC alleged that Internet marketer Jumpstart Technologies disguised commercial email messages to appear as personal messages from friends and misled consumers as to the terms and conditions of its "free" movie ticket promotions. To resolve those allegations, the company paid $900,000, the largest civil penalty obtained under the CAN-SPAM Act.[19] Deceptive spam also can be part of a scheme that is

---

[16] *See, e.g.*, *FTC v. Pereira*, No. 99 Civ. 562 (E.D.N.Y.) (Final Order Jan. 24, 2005), www.ftc.gov/opa/1999/09/atariz.htm (pagejacking); *FTC v. Hill*, No. H 03-5537 (S.D. Tex.) (Stipulated Final Order May 24, 2004), www.ftc.gov/opa/2004/03/ phishinghilljoint.htm (phishing); and *FTC v. Sheinkin*, No. 2-00-3636-18 (D.S.C.) (Stipulated Final Order Aug. 15, 2001), www.ftc.gov/opa/2001/08/ sheinkin.htm (modem hijacking).

unique to the Internet. For example, in one case the FTC alleged that a defendant's email messages claimed that consumers won a Sony PlayStation in order to lure consumers to an adult website and surreptitiously redirect their Internet connections through a 900-number that charged them up to $3.99 a minute for the new connection.[20]

The FTC also has taken law enforcement actions against distributors of spyware – another technology-driven scheme that provides digital data thieves with a back door into consumers' online lives. Spyware is downloaded without authorization and may be used to send high volumes of pop-up ads, redirect computers to unwanted websites, monitor Internet surfing, or record consumers' keystrokes, which, in turn, could lead to identity theft. In the past three years, the Commission has filed 11 cases against purveyors of spyware, disgorging over $12.9 million of their alleged ill-gotten gains. In the Commission's most recent spyware case, the FTC alleged that Direct Revenue, LLC surreptitiously installed advertising software programs, which monitored Internet use to display targeted pop-up ads on consumers' computers, and deliberately made the programs difficult for consumers to identify and remove. To settle these charges, Direct Revenue agreed to disgorge $1.5 million and to abide by injunctive provisions that will protect consumers from these practices in the future.[21]

The FTC employs a number of tools to develop its cases targeting online fraud. For example, the Commission identifies potentially violative commercial email through its spam database. Each day, the FTC receives approximately 300,000 pieces of spam – forwarded by

---

[20] *FTC v. BTV Indus.*, No. CV S-03-1306 (D. Nev.) (Stipulated Final Order Nov. 25, 2003), www.ftc.gov/opa/2004/02/playstation2.htm.

[21] *In re DirectRevenue, LLC*, FTC File No. 052-3131 (Consent Agreement Feb. 16, 2007), www.ftc.gov/opa/2007/02/directrevenue.htm.

computer users to spam@uce.gov – and stores it in a large database, which currently houses more than 400 million pieces of unsolicited commercial email, including emails regarding apparently bogus health claims.

The FTC's Consumer Sentinel database also plays a central role in the agency's law enforcement efforts. The Consumer Sentinel database contains over 3.7 million consumer fraud and identity theft complaints filed with the FTC; other federal, state, and local law enforcement agencies; and private organizations. The FTC, as well as more than 1,600 law enforcement entities worldwide, use the database to identify scams, specific companies generating high levels of complaints, and individual consumers who may have been harmed by illegal activity.[22]

In addition, the recently-enacted US SAFE WEB Act[23]

consumer witnesses, and money derived from scams are located in foreign countries. To help overcome the challenges of investigating and prosecuting these types of international fraud, the US SAFE WEB Act strengthens the FTC's ability to cooperate with its foreign counterparts, gather information from international sources, and follow the money trail without tipping off the fraud's perpetrators.

As with health-related fraud, the FTC combines its law enforcement efforts against all types of Internet fraud with consumer education and business outreach campaigns. The FTC has produced a wide array of materials to educate consumers on how to spot and avoid online scams and to increase business awareness on how to comply with the law. For example, the award-winning website, OnGuardOnline.gov, contains tips, articles, videos, and interactive materials to educate consumers on guarding against Internet fraud, filter spam, secure their computers, and protect their personal information. The FTC developed OnGuardOnline in conjunction with industry partners and other agencies, and since its launch in late 2005, the site has attracted more than 3.5 million visits. The FTC also disseminates a variety of business education materials, including materials to inform businesses about complying with the CAN-SPAM Act,[24] and publications providing advice on making clear disclosures in online ads.[25]

IV. Conclusion

The FTC has been involved in policing the Internet for more than a decade and will continue to protect consumers from the various types of online fraud. As technology and scams change, the Commission continues to shift its resources to target those frauds that cause the most

---

[24] *See* www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm.

[25] *See* www.ftc.gov/bcp/conline/pubs/buspubs/dotcom/index.pdf.

harm to consumers. In addition, the FTC will continue its efforts to ensure the truthfulness and accuracy of advertising for health-related products, regardless of the medium in which the ads appear. This includes efforts against deceptive advertising targeted toward older Americans, who are among our most vulnerable populations. Thank you for providing the Commission an opportunity to appear before the Committee.