

PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION ON

"INTERNET FRAUD"

Before the

SUBCOMMITTEE ON COMMERCE, TRADE,
AND CONSUMER PROTECTION
of the
COMMITTEE ON ENERGY AND COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

May 23, 2001

Mr. Chairman, I am Eileen Harrington, Associate Director of the Division of Market Practices in the Federal Trade Commission's Bureau of Consumer Protection. At the Committee's request, my remarks will focus primarily on the FTC's efforts to combat fraud on the Internet. I will also touch on two other specific areas of concern both to the Committee and the Commission, namely, identity theft and "pretexting."

Fraud- whether on the Internet or in the "brick and mortar" world - probably needs little explanation, but it may be useful to clarify what the terms "identity theft" and "pretexting" signify. Identity theft is the use by a thief, unbeknownst to his victim, of the victim's name, social security number or other personal identifying information, to open accounts, rack up huge debts for goods and services. Identity theft certainly predates the Internet and although identity thieves are finding ways to exploit this new medium, this pernicious practice utilizes rather primitive means, such as intercepting a victim's mail, or scavenging personal information from a victim's trash. "Pretexting" a term coined by the private investigation industry, and refers to the practice of obtaining personal information under false pretenses. For example, an investigator who obtains a bank account balance by posing as the account holder would be engaged in pretexting. This tactic is perhaps as old as the private investigation industry itself. But it appears to be gaining in popularity- especially in the burgeoning Internet marketplace because of the booming market for comprehensive personal information.

I. Introduction and Background

A. The FTC and its Law Enforcement Authority

The FTC is the federal government's primary consumer protection agency. While other federal agencies have jurisdiction over a specific market sector, the Commission's jurisdiction extends over nearly the entire economy, including business and consumer

transactions on the Internet⁽²⁾.

Under the Federal Trade Commission Act⁽³⁾, the agency's mandate is to take action ag

C. The FTC's Response to Protecting Consumers in the Online Marketplace

Stretching its available resources to combat the growing problem of Internet fraud and deception, the Commission has targeted a wide array of online consumer protection problems. This effort has produced significant results. Since 1994, the Commission has brought 182 Internet-related cases against over 593 defendants. It obtained injunctions stopping the illegal schemes,

consumer complaint data from its central fraud database with Consumer Sentinel.

The Commission provides secure access to this data over the Internet, free of charge to over 300 U.S., Canadian, and Australian law enforcement organizations including the Department of Justice, U.S. Attorneys' offices, the Federal Bureau of Investigation, Securities and Exchange Commission, the Secret Service, the U.S. Postal Inspection Service, the Internal Revenue Service, the offices of all 50 state Attorneys General, state sheriffs and prosecutors, the Royal Canadian Mounted Police, and the Australian Competition and Consumer Commission. Consumer Sentinel is a dynamic online law enforcement tool to use against all types of fraud, especially online fraud.

The central role that Consumer Sentinel plays in the Commission's law enforcement efforts is exemplified by "Operation Top Ten Dot Cons," the Commission's latest broad "sweep" of fraudulent and deceptive Internet scams. In a major law enforcement effort, the FTC Inspection

solicitations. Sites that continue to make unlawful claims are targeted for possible enforcement action.

To date, the Commission has conducted 27 different Surf Days targeting problems ranging from "cure-all" health claims to fraudulent business opportunities and credit repair scams.⁽²²⁾

More than 250 law enforcement agencies or consumer organizations around the world have joined the Commission in these activities; collectively, they have identified over 6,000 Internet sites making dubious claims. The law enforcement Surf Day has proved effective that it is now widely used by other government agencies, consumer groups and other private organizations.

B. Traditional Scams Use the Internet to Expand in Size and Scope

Out of the 170 cases brought by the Commission against Internet fraud and deception, over half have targeted old-fashioned scams that have been retooled for the new medium. For example, the Commission has brought 28 actions against online credit repair services, 25 cases against deceptive business opportunities and MLM schemes, and 11 cases against pyramid schemes.

It is no surprise that the Internet has become a major tool for scammers that it is now widely used by other government agencies, consumer groups and other private organizations.

injunction shutting down the scheme, barring for life the scheme's principals from a multi-level marketing business, and ordering them to pay \$2.9 million in consumer redress.

C. Scams Are Increasingly HighTech.

Although most Internet fraud stems from traditional scams, the number of schemes uniquely and ingeniously exploiting new technology is multiplying. These are the most insidious schemes because they feed on the public's fascination and suspicion of new technology. Their ultimate effect can only be to undermine consumer confidence in the online marketplace. To combat this type of high fraud, the Commission has supported staff training and given its staff the tools to be effective-sleuths.

Recognizing that most of its attorneys and investigators need to be Internet savvy, the Commission has hosted beginner and advanced Internet training seminars and sessions on new technology, investigative techniques, and Internet case law. The Commission also makes this training available to personnel of other law enforcement agencies. In the past year, the Commission has presented Internet training seminars in seven U.S. cities and in Toronto, Canada, and Paris, France. In addition to FTC staff, these sessions trained approximately 800 individual participants from other law enforcement agencies. These participants represented twenty different countries in the U.S., twenty-six states, twenty-two federal agencies, and fourteen Canadian law enforcement agencies. Among those who have participated are representatives from the offices of state Attorneys General, the Department of Justice and U.S. Attorneys, the Securities and Exchange Commission, the FBI, and the Postal Inspection Service.

In addition to providing regular Internet training, the Commission also provides its staff with the tools they need to investigate high fraud. The FTC's Internet Lab is an important example. With high speed computers that are separate from the agency's network and equipped with current hardware and software, the Lab allows staff to investigate fraud and deception in a secure environment and to preserve evidence

incur charges on the line for such service. Once downloaded and executed, however, the program actually hijacked the consumer's computer modem by surreptitiously disconnecting the modem from the consumer's local Internet Service Provider, dialing a high-priced international long distance call to Madagascar, and reconfiguring the consumer's modem to the Internet from some overseas location, opening at an adult site. The line subscriber the consumer responsible for paying phone charges on the line -- then began incurring charges on his or her phone lines for the remote connection to the Internet at the rate of \$3.99 per minute. The court has ordered a preliminary injunction in this matter, and litigation continues.⁽²⁸⁾

2. "Pagejacking" and "Mousetrapping"

Earlier, in *FTC v. Carlos Pereira d/b/a atariz.com*,⁽²⁹⁾ the Commission attacked a world wide, high-tech scheme that allegedly "pagejacked" consumers and then "mousetrapped" them at adult pornography sites. "Pagejacking" is making exact copies of someone's Web page, including the imbedded text that informs search engines about the subject matter of the site. The defendants allegedly made unauthorized copies of millions of pages from other Web sites, including those of Paine Webber and the Harvard Law Review. The defendants made one change on each copied page that was hidden from view: they inserted a command to "redirect" any surfer coming to the site to another Web site that contained sexually explicit, adult-oriented material. Internet surfers searching for subjrn '12 88.dsuc6

uncovered by the sting, the FTC filed complaints alleging that the defendants ranging from \$100 to \$600 would obtain bank account balances by calling a bank and pretending to be the customer.

The courts in all three cases immediately entered TROs to halt the illegal activity, freeze certain of the defendants' assets, and require the defendants to produce their financial business records to the Commission. Shortly thereafter, all three defendants stipulated to preliminary injunctions continuing the relief granted in the TROs. The Commission's order is an order permanently barring defendants' illegal pretexting practices and disgorging money defendants earned from them.

E. Online Scams Spread Quickly and Disappear Quickly.

One hallmark of Internet fraud is the ability of perpetrators to cover their tracks and mask their locations and identities. Using anonymous emails, hidden Web sites, and falsified domain name registrations, many fraud operators are able to strike quickly and victimize thousands of consumers in a short period of time, and disappear nearly without trace.

To stop these swift and elusive con artists, law enforcement must move just as fast. The FTC's Internet Rapid Response Team was created for this very purpose. It draws heavily upon complaints collected by the FTC's Consumer Response Center and the Consumer Sentinel system. The team constantly reviews complaint data to spot emerging problem conduct quick but thorough investigations, and prepare cases for filing in federal courts. Based on such data review, FTC staff had completed its investigation and was in court successfully arguing for an *ex parte* temporary restraining order and asset freeze in *Verity International, Ltd.* within a little more than a week after the first complaints began coming in to the Consumer Response Center.

In another exemplary effort, *FTC v. Benoit*,⁽³⁵⁾ the Rapid Response Team quickly moved against defendants who allegedly used deceptive emails or "spam" to dupe consumers placing expensive international audiotext calls. The defendants allegedly sent thousands of consumers an email stating that each recipient's "order" had been received and that his or her credit card would be billed \$250 to \$899. The email instructed consumers to call a telephone number in the 767 area code if they had any questions. Consumers did not realize that 767 was the area code for Dominica, West Indies. When consumers called the number expecting to reach a customer representative, they were connected to an audiotext entertainment service with sexual content and charged expensive international rates.⁽³⁶⁾

Even though a string of telephone carriers could not identify who operated the audiotext number in question, the Internet Rapid Response Team constructed a compelling case about three weeks. The Commission quickly obtained a federal court order to stop the scheme and freeze any proceeds of the fraud still in the telephone billing system.

F. Effective Remedies Are More Difficult to Achieve in the Global Online Market.

The globalization of the marketplace poses new and difficult challenges for consumer protection law enforcement. Anticipating this development, the Commission held public hearings in the fall of 1995 to explore business and consumer issues arising from technological innovation and increasing globalization. Over 200 companies, consumer business representatives, legal scholars, consumer advocates, and state and federal officials presented testimony, and the Commission published a volume report summarizing the testimony and the role of antitrust and consumer protection law in a changing marketplace. As reported in, "Anticipating the 21st Century: Consumer Protection in the New High Tech, Global Marketplace," there was a broad consensus that meaningful consumer protection takes: (1) coordinated law enforcement against fraud and deception; (2) private initiatives and public/private partnerships; and (3) consumer education through the combined efforts of government, business, and consumer groups.⁽³⁷⁾ These principles have guided FTC policy regarding the Internet ever since.

In addition to gathering information through hearings and workshops, the FTC has gained practical knowledge about the effects of globalization and e-commerce through its litigation. In this respect, the Commission has found that pursuing Internet fraud often involves a difficult and costly search for money that has been moved offshore. For example, in *FTC v. J.K. Publications*,⁽³⁸⁾ the defendants, who had made unauthorized charges of \$19.95 per month on consumers' credit or debit cards for purported Internet services, moved much of their ill-gotten gains offshore. The Commission ultimately won a \$37.5 million verdict in this matter, but in the course of litigation, the receiver appointed in this case reported that the defendants had moved millions of dollars to the Cayman Islands, Liechtenstein, and Vanuatu in the South Pacific. However, to date, despite substantial litigation costs, the monies have not been fully repatriated.⁽³⁹⁾

In addition to fraud proceeds moving offshore more quickly, fraudulent online operators may be beyond the reach of the Commission and U.S. courts, practically if not legally. The limited recognition of civil judgments from country to country. Even if the Commission were to bring an action and obtain a judgment against a foreign firm that has defrauded U.S. consumers, the judgment might be challenged in the firm's home country and the ability to collect any consumer redress might be frustrated. In light of this possibility, U.S. law enforcement must look

for more effective crossborder legal remedies, and must work more cooperatively with law enforcement and consumer protection officials in other countries.

To meet this challenge, the Commission is increasingly cooperating with international counterparts in a number of venues. One is the International Marketing Supervision Network (IMSN), a group of consumer protection agencies from the 30 countries that are members of the Organization for Economic Cooperation and Development (OECD). The FTC has also executed cooperation memoranda with agencies in Canada, the United Kingdom, and Australia.

In addition to placing publications on its own Web site, the FTC actively ~~engages~~
~~partners~~ government agencies, associations, organizations, and corporations with an
interest in a particular subjecto link to its information from their sites and to place

1999.⁽⁴²⁾ The FTC continues to maintain the site.

E. Business Education for Online Marketers

As part of its mission, the FTC provides guidance to marketers on how to assure that basic consumer protection principles apply online. Many of these entrepreneurs are small, startup companies that are new to the Internet and to marketing in general and are unfamiliar with consumer protection laws. The Commission's publication, *Advertising and Marketing on the Internet: Rules of the Road*, is designed to give practical, plain-English guidance to them.⁽⁴³⁾ FTC also has used a variety of other approaches to get its messages out to the business community, from posting compliance guides, staff letters and banner public service announcements on the Web to speaking at industry academic meetings and conferences, using trade press to promote the availability of information on the agency site, and holding workshops on online issues and posting transcripts. Most recently, on January 30 of this year, the Commission, in cooperation with the Electronic Retailing Association, presented "Etail Details," a seven-hour Internet marketing seminar for Internet retailers, marketers, and suppliers on applying off-line and regulations online. The seminar was designed to ensure retailers understand and comply with FTC rules regarding e-tailing.

IV. Conclusion

The Commission has been involved in policing the electronic marketplace for more than six years before the World Wide Web was widely used by consumers and businesses. The Commission has strived to keep pace with the unprecedented growth of the e-marketplace by targeting our efforts, making innovative use of the technology, and leveraging our resources to combat fraud on the Internet. In addition, the Commission has taken the necessary steps to fulfill its responsibilities under both the Identity Theft Assumption and Deterrence Act of 1998 and, with respect to pretexting, the Gramm Leach Bliley Act to promote protection of consumers' personal financial information by financial institutions. We have done this within the framework of limited resources, without retreating from our important consumer protection work in traditional markets.

The Commission greatly appreciates the opportunity to describe its efforts to combat fraud on the Internet, and its activities against identity theft and pretexting.

Endnotes:

1. The views expressed in this statement represent the views of the Commission. My responses to questions you may have are my own and not necessarily those of the Commission or any Commissioner.
2. The FTC has limited or no jurisdiction over specified types of entities and activities. These include savings associations, and federal credit unions; regulated common carriers; over-the-counter retail sales of livestock and meat products under the Packers and Stockyards Act; certain activities of nonprofit corporations; and the business of insurance. See, e.g., 15 U.S.C. §§ 44, 45, 46 (FTC Act); 15 U.S.C. § 281 (Clayton Act); 7 U.S.C. § 227 (Packers and Stockyards Act); 15 U.S.C. § 101 *et seq.* (McCarran-Ferguson Act).

3. 15 U.S.C. § 5(a). The Commission also has responsibilities under more than 45 additional statutes, including the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*, which establishes important privacy protections for consumers' sensitive financial information; the Truth in Lending Act, 15 U.S.C. § 1601 *et seq.*

no more new recruits can be found, these schemes collapse and a vast majority of participants lose money they invested.

24. To date, the Commission has collected about \$42.6 million in these cases.

25. *FTC v. Fortuna Alliance, L.L.C.*, No. C96799M (W.D. Wash. 1996). *See also, FTC v. JewelWay International, Inc.*, No. CV97383 TUC JMR (D. Ariz. 1997) (\$5 million in redress for approximately 150,000 investors); *FTC v. Nia Cano*, No. 97-7947-CAS-(AJWx) (C.D. Cal. 1997) (approximately \$2 million in redress); *FTC v. FutureNet*, No. 98-1113GHK (AIJx) (C.D. Cal. 1998) (\$1 million in consumer redress); *FTC v. Five Star Auto Club, Inc.*, 97 F. Supp. 2d 502 (S.D.N.Y. 2000). (\$2.9 million in consumer redress); *FTC v. Equinox International Corp.*, No CV-S-990969JBR-RLH (D.Nev. 1999) (pyramid promoted through many devices, including some use of the Internet; \$50 million in consumer redre

26. *FTC v. Five Star Auto Club, Inc.*, 97 F. Supp. 2d 502 (S.D.N.Y. 2000).

27. *FTC v. Verity International* 6n6n6n6,-3(I3(r)3 0 0 9.96 103.68 528.48 Tm 2(ofF./ttj 0.d)12(7)12(F)8(.)3(S.68 554.04 Tm [(F

In the course of the litigation, Commission attorneys were able to identify the operators of the scheme.

36. "Audiotext" services are telephone-based entertainment or information services.

37. See Bureau of Consumer Protection, Federal Trade Commission, *Anticipating the 21st Century: Consumer Protection in the New High-Tech, Global Marketplace*, iii (May 1996); See also, *Looking Ahead: Consumer Protection in the Global Electronic Marketplace* (September 2000).

38. *FTC v. J.K. Publications*, No. 99000-44ABC (AJWx)(C.D. Cal. 1999).

39. Similarly, in *FTC v. Fortuna Alliance*, the Commission found that the defendants had transferred \$2.8 million to Antigua, West Indies. With the assistance of the U.S. Department of Justice's Office of Foreign Litigation, the Commission obtained an order from an Antiguan court freezing those funds and a stipulated judgment in U.S. court that required the defendants to repatriate that money for consumer redress. However, it cost \$280,000 in fees alone to litigate the case in foreign court. In this case, the Department of Justice's Office of Foreign Litigation paid \$50,000 up front, and the U.S. court ordered the defendants to pay the remaining \$230,000 in fees. In other cases, the Commission may have to bear all or most of the cost of litigating in foreign court.

40. With respect to identify theft, the Commission also conducts an extensive media education campaign including print materials, media mailings and videos and a website, located at www.consumer.gov/idtheft. The FTC's consumer education booklet, *Identity Theft: When Bad Things Happen to Your Good Name*, covers a wide range of topics, including how identity theft occurs, how one can protect one's personal information and minimize their risk, what steps to take immediately upon one is a victim, and how to correct credit and other problems that may result from identity theft. It also describes federal and state resources that are available to consumers who have particular problems as a result of identity theft. The FTC has distributed directly more than 230,000 copies of the booklet through April 2001. Another 425,000 copies have been printed and are being distributed by the Social Security Administration. The identity theft website includes the booklet, descriptions of common identity theft