PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION ON

"INTERNET FRAUD"

Before the

SUBCOMMITTEE ON INVESTIGATIONS

of the

GOVERNMENTAL AFFAIRS COMMITTEE

UNITED STATES SENATE
Washington, D.C.

February 10, 1998

Madam Chairman and members of the Committee: I am Robert Pitofsky, Chairman of the Federal Trade Commission ("FTC" or "Commission"). I appreciate this opportunity to present the Commission's views on the important issue of fraud on the Internet.[(1)]

Introduction

The Commission pursues its mission of promoting the efficient functioning of the marketplace by seeking to protect consumers from unfair or deceptive acts or practices and to promote vigorous competition. As you know, the Commission's responsibilities are far-reaching. Its primary legislative mandate is to enforce the Federal Trade Commission Act, which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[(2)] With the exception of certain industries, this statute provides the Commission with broad law enforcement authority over virtually every sector in our economy;[(3)] commerce on the Internet falls within the broad sweep of this statutory mandate.

The advent of the Internet -- with its new methods of communicating through web sites, electronic mail, news groups, chat rooms, electronic bulletin boards, and commercial on-line services -- is an historical development much like the introduction of television or, a few generations earlier, the telephone. Like these earlier technologies, the Internet presents consumers with an exciting new means for them to purchase both innovative and traditional goods and services faster and at lower prices, to communicate more effectively, and to tap into rich sources of information that were previously difficult to access and that now can be used to make better-informed purchasing decisions.

The Internet's promise of substantial consumer benefits is, however, coupled with the potential for fraud and deception. Fraud is opportunistic, and fraud operators are always

among the first to appreciate the potential of a new technology. This phenomenon was illustrated by the advent, flourishing, and near-demise of pay-per-call (900-number) technology as a commercial medium during the last decade. 900-number technology was the first interactive technology -- and still is the only interactive technology offering nearly universal access because all that is needed is a telephone. This technology has huge potential as an alternative payment system, since every telephone could serve as a payment terminal, and no credit cards, debit cards, or checks are needed. In 1991, there were $6 billion in pay-per-call transactions. But fraud operators moved in to exploit the technology, and the industry was slow to respond to this challenge. As a result, the 900-number industry's reputation became tarnished by fraud and abuse, and sales plummeted to $300 million annually. In 1992, pursuant to Congressional mandate, the FTC and the FCC promulgated rules to regulate the 900-number industry to ensure that consumers would receive price and other material information before incurring costs, and have the right to dispute allegedly incorrect or unauthorized charges.[(4)] Annual sales began to climb again, reaching $450 million in 1995. The 900-number industry now seems poised to attract a higher volume of legitimate commerce because consumers can use 900-numbers with greater confidence.

Some of the same features that made pay-per-call technology a tempting field for fraud artists in the 1980s -- low start-up costs and the potential for big profits -- exist on the Internet today. Indeed, after buying a computer and modem, scam artists can establish and maintain a site on the World Wide Web for $30 a month or less and solicit consumers anywhere on the globe. There is nothing new about most types of Internet fraud the Commission has seen to date. What is new -- and striking -- is the size of the potential market and the relative ease, low cost, and speed with which a scam can be perpetrated.

If the Internet is to avoid a fate similar to that of 900-number technology, the Commission believes it is important to address Internet fraud now, before it discourages new consumers from going on-line and chokes off the impressive commercial growth now in progress and potential for innovation on the Internet. According to some industry analysts, total Internet business will climb from $2.6 billion in 1996 to $220 billion by 2001.[(5)] Much of this trade likely will involve business-to-business transactions. However, the on-line consumer market also is growing, and at an exponential rate. In early 1997, 51 million adults were already on-line in the U.S. and Canada.[(6)] Of those people, 73% reported that they had shopped for product information on the World Wide Web, the interactive graphics portion of the Internet.[(7)] By December 1997, the number of on-line users had risen to 58 million adults in the U.S. and Canada, and 10 million had actually purchased a product or service on-line.[(8)] Perhaps most telling, analysts estimate that Internet advertising -- which totaled approximately $301 million in 1996 -- will reach $4.35 billion by the year 2000.[(9)]

If this trend and all the benefits that it implies are to continue, consumers must feel confident that the Internet is safe from fraud. Nothing is more likely to undermine their confidence than exploitation by scam artists using this new technology as yet another means to defraud consumers. Therefore, the Commission, like the Subcommittee, is

concerned about fraud on the Internet and has taken strong action to combat it.

The Commission began to examine the potential for consumer protection problems on the Internet proactively, before on-line consumer transactions became common. In the fall of 1995, the Commission held public hearings to explore business and consumer issues arising from technological innovation and increasing globalization. Over 200 company executives, business representatives, legal scholars, consumer advocates, and state and federal officials presented testimony. A two-volume report was published summarizing the hearings. Volume II, "Anticipating the 21st Century: Consumer Protection in the New High-Tech, Global Marketplace," reflects principles that many participants urged the Commission to consider when addressing the Internet and other technologies in the new Information Age:

Consumer protection is most effective when businesses, government, and consumer groups all play a role. 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.[(10)]

Applying these principles, the Commission has taken the offensive against fraud on the Internet through a three pronged-strategy that emphasizes targeted law enforcement action, complemented by education of consumers and new Internet entrepreneurs, both of whom may be venturing into cyberspace for the first time. In all aspects of this strategy, but particularly in the Commission's consumer and business education efforts, the Commission has sought to form new partnerships with private industry and other government agencies, and the Commission has tried to turn new technologies to our advantage.

Law Enforcement

First and foremost, the FTC is a civil law enforcement agency with strong and effective enforcement tools to combat fraud and deception. The Commission can issue administrative complaints and conduct administrative adjudications that may result in the issuance of cease and desist orders against practices found to be unfair or deceptive.[(11)] Further, in cases of fraud and other serious misconduct, the Commission has statutory authority to file suit directly in federal district court to obtain preliminary and permanent injunctive relief, redress for injured consumers, or disgorgement of ill-gotten gains.[(12)] The Commission also may seek the assistance of the Department of Justice in filing criminal contempt proceedings against persons who violate court orders issued at the behest of the Commission, or in filing criminal actions in egregious fraud cases.

The Commission has brought over 25 law enforcement actions against defendants whose alleged illegal practices used or involved the Internet. Several of these cases involved alleged deceptive advertising and billing practices of commercial on-line service providers.[(13)] Most of the Commission's law enforcement actions, however, have involved old-fashioned scams dressed up in high-tech garb.[(14)] For example, the Commission has

brought several cases to stop alleged pyramid schemes that recruit victims through the web.[(15)] In the Commission's largest Internet pyramid case to date, *FTC v. Fortuna Alliance*,[(16)] the defendants allegedly promised consumers that, for a payment of $250, they would receive profits of over $5,000 per month. The program spawned numerous web sites on the Internet and appealed to victims all around the globe seeking to get rich quickly for little effort. Yet sheer mathematics dictated that 95 percent of the consumers who joined the program could never make more than they paid in. The Commission obtained a temporary restraining order halting the unlawful practices and freezing the assets of the individuals who developed and operated the Fortuna program. The court order also required the defendants to repatriate the assets they had deposited overseas. In February 1997, the defendants stipulated to a permanent injunction that prohibited their alleged pyramid program and provided for redress to consumers who requested refunds. The defendants subsequently balked at paying many consumers, and the Commission filed a contempt motion. The court did not impose sanctions but issued a compliance order against the defendants on January 6, 1998. The compliance order clears the way for over 8,600 Fortuna members to begin receiving refunds.

Another alleged Internet pyramid scheme targeted in a recent Commission law enforcement action was Credit Development International.[(17)] The scheme was propelled by allegedly false promises that those who joined CDI would receive an unsecured Visa or MasterCard credit card with a $5,000 limit and a low interest rate, as well as the opportunity to receive monthly income of $18,000 or more. The Commission filed its complaint on October 29, 1997, and on October 31, the court granted a temporary restraining order, appointed a receiver to oversee the corporate defendants, and froze both the corporate and individual defendants' assets. After a hearing, on November 20, 1997, the court issued a preliminary injunction against the defendants. The Commission's staff estimates that over 30,000 consumers collectively may have lost 3 to 4 million dollars in this alleged scam. This matter is still in litigation.

The Commission's investigators discovered the Credit Development International scam as part of an ongoing effort to monitor "spam" -- also known less colloquially as unsolicited commercial e-mail ("UCE") -- on the Internet. One theme sounded in the Commission's recent privacy hearings was that an ever-increasing volume of UCE strains the capacity of on-line service providers and threatens the development of the Internet as a conduit for commerce. For example, at the Commission's privacy hearings held in June 1997, America Online ("AOL") reported that it handled 15 million electronic messages per day. By September 1997, that number had quadrupled to 60 million messages per day. Significantly, AOL has estimated that UCE comprises as much as one-third of all e-mail traffic.

Beyond the sheer volume and potential annoyance of UCE, many UCE messages may be misleading or deceptive.[(18)] Alleged scams like Fortuna and Credit Development International generate huge quantities of UCE, because e-mail is unparalleled as a means of cultivating a "downline" -- additional recruits to a pyramid -- for virtually no cost and little effort. The same attributes make UCE attractive to other types of scams as a means

to solicit millions of consumers for little cost.

Although most Internet fraud is fairly traditional, the Commission has taken action against one scheme that uniquely and ingeniously exploited what can be done on the Internet and *only* on the Internet. The case *FTC v. Audiotex Connection, Inc*., CV-97 0726 (DRH) (E.D.N.Y.), presented a scheme that allegedly "hijacked" consumers' computer modems by surreptitiously disconnecting them from their local Internet Service Provider (such as AOL) and reconnecting them to the Internet through a high-priced international modem connection, purportedly going to Moldova but actually terminating in Canada. On various Internet sites, the defendants offered access to free computer images through a special "viewer" program. If a consumer downloaded and activated the viewer software, the alleged hijacking automatically ensued, and an international long-distance call (and the charges for it) continued until the consumer turned off the computer -- even if he or she left defendants' sites and moved elsewhere on the Internet, or left the Internet entirely to use a different computer program.

Commission staff were first alerted to the *Audiotex* scheme by security experts at AT&T. The United States Secret Service assisted staff in ascertaining how this "Trojan horse" viewer software worked, and AT&T lent further assistance in tracing the software back to specific web sites. With this help, the Commission's staff completed its investigation, filed a complaint, and obtained an *ex parte* temporary restraining order and asset freeze against the defendants within just 31 days of learning about the alleged scam. The lawsuit was recently resolved by entry of a stipulated permanent injunction against the main defendants named in the Commission's complaint and the issuance of a virtually identical administrative order against additional parties found to have played a role in the alleged scam. Under the two orders, the defendants and administrative respondents are barred from engaging in the alleged unlawful practices, and over 38,000 consumers should receive full redress worth an estimated $2.74 million.[(19)]

Consumer Education

The Commission has gone on-line to reach Internet users. Since April 1995, the Commission has used its web site at "www.ftc.gov" to make instantly available to consumers a rich and continuously updated body of advice and information. The Commission receives approximately 60,000 to 75,000 "hits" per day on this home page.[(20)] In September 1997 alone, FTC.GOV received almost 2 million hits from 114,000 visitors.

In constructing its web site, the Commission has put a premium on making it not only comprehensive, but also user-friendly. FTC.GOV contains a search engine that allows consumers to pull up information by typing in a few key words. The site also contains a special section called ConsumerLine that provides news releases, consumer alerts, and on-line versions of all of the Commission's consumer and business education publications.[(21)]

Building on the success of the FTC's home page, the Commission's staff conceived a plan

to create a new site at "www.consumer.gov" and has developed the site in partnership with sister agencies -- the Securities and Exchange Commission ("SEC"), the U.S. Consumer Product Safety Commission ("CPSC") the Food and Drug Administration ("FDA"), and the National Highway Traffic Safety Administration ("NHTSA"). CONSUMER.GOV provides the public with "one-stop shopping" for federal information on a broad spectrum of consumer issues, ranging from auto recalls to drug safety to investor alerts.[(22)]

Extending a hand to consumers at their most vulnerable point -- when they are surfing in areas of the Internet likely to be rife with fraud and deception -- the staff of the Commission has posted several "teaser" web sites. The "Ultimate Prosperity Page" is one example advertising a fake deceptive business opportunity. The "Ultimate Prosperity Page" uses "buzz words" and promises of easy money common to many such scams. When the consumer clicks from the "Ultimate Prosperity Page" to the next page in the series, he or she finds glowing testimonials from fictitious persons who purportedly have achieved fabulous success through the business opportunity -- again mirroring the typical get-rich-quick business opportunity scam. Clicking through to the third and final page in the series, however, brings the consumer to a sobering warning: "If you responded to an ad like [this], you could get scammed." The warning page gives advice on how to avoid fraudulent business opportunities and provides a hyper-text link back to FTC.GOV, where consumers can learn more about investing in franchises or business opportunities.[(23)]

There are now other teaser sites, posted by the Commission's staff, that mimic pyramid schemes, scholarship scams, deceptive travel programs, false weight-loss claims, and fraudulent vending opportunities -- all perennial frauds that have been practiced on consumers for years through direct mail, telemarketing, and other means, and are now enjoying new life on the Internet.[(24)] The Commission's staff has registered each "teaser" site with major search engines and indexing services on the Internet. Thus, consumers may encounter the site when they are perhaps most receptive, just when they may be about to become ensnared in a fraud by responding to a plausible but untrue come-on. Private on-line service companies have worked with the Commission's staff to highlight various teaser pages and have billed some as the "new" or "cool" site of the week.[(25)]

In another effort to use new technology to reach the public, the staff of the Commission partnered with the North American Securities Administrators Association and held a real time on-line forum on the Internet in April 1997. Over 100 consumers participated, posing questions to, and receiving instantaneous responses from, state and federal experts about how to invest wisely in new business ventures or franchises. The Commission posted the transcript of this "chat" session on its web site so that other consumers could access it and benefit from the exchange.

The Commission has actively sought Internet companies and trade groups to join with us as partners in disseminating consumer protection information to consumers on-line. As a result, the Interactive Services Association, a leading on-line trade association, and companies such as AT&T, NetCom, and America Online have helped circulate public

service announcements over the Internet, cautioning consumers to avoid particular scams and "hot linking" consumers to the Commission's web site where they can find "Cybershopping" guides, "Safe Surfing" tips, and other helpful information.

Business Education

At the forefront of its business education efforts, the Commission has conducted a number of "Surf Days" aimed at providing information to new entrepreneurs who may unwittingly violate the law. The first Surf Day was conducted in December 1996 and focused on pyramid schemes that had begun to proliferate on the Internet. Commission attorneys and investigators enlisted the assistance of the SEC, the U.S. Postal Inspection Service, the Federal Communications Commission, and 70 state and local law enforcement officials from 24 states. This nation wide *ad hoc* task force surfed the Internet one morning, and in three hours, found over 500 web sites or newsgroup messages promoting apparent pyramid schemes. The Commission's staff e-mailed a warning message to the individuals or companies that had posted these solicitations, explaining that pyramid schemes violate federal and state law and providing a link back to FTC.GOV for more information. In conjunction with the New York Attorney General's Office and the Interactive Service Association, the Commission announced the results of Internet Pyramid Surf Day at a televised press conference held during the Internet World '96 convention in New York City. A month later, the Commission's investigative staff checked on the status of web sites or newsgroups identified as likely pyramids during Surf Day and found that a substantial number had disappeared or been improved.[(26)] The Commission has employed this technique several times since, conducting additional Surf Days focused on Internet web sites or newsgroup messages that promoted potentially problematic business opportunities, credit repair schemes, and "miracle cure" health products.

The Commission has now taken its Surf Day concept to the private sector, the global law enforcement community, and sister agencies as well. In August 1997, the Coupon Information Center, a private trade association, and its members from the national merchandising community joined Commission staff in surfing for fraudulent opportunities that promoted coupon certificate booklets. Then on October 16, 1997, the Commission helped coordinate the first "International Internet Surf Day." Agencies from 24 countries joined this effort and targeted "get-rich-quick" schemes on the Internet.[(27)] Australia's Competition and Consumer Commission oversaw the world-wide effort while the FTC led the U.S. team consisting of the SEC, the Commodities Futures Trading Commission ("CFTC") and 23 state agencies.

In November 1997, the Commission used the Surf Day concept to help the Department of Housing and Urban Development ("HUD") target unscrupulous "HUD Tracers." These "tracers" track down consumers to whom HUD may owe a refund for FHA mortgage insurance. Consumers can claim their refund for free by contacting HUD directly; however, unscrupulous "tracers" may falsely claim that refunds cannot be secured without their assistance (and they may charge up to 30 percent in commissions), may falsely claim an affiliation with the government, and may falsely represent to other

entrepreneurs how much money they can make as "HUD tracers." The HUD Tracer Surf Day not only helped to generate publicity to inform consumers about HUD's refund program, but it also helped eliminate many potentially deceptive solicitations from the Internet. A month after sending out warning messages, the Commission's staff checked on suspect tracer sites and found that 70 percent had shut down entirely or removed questionable claims about earnings potential or their affiliation to HUD.

Earlier this month, the Commission announced yet another innovative use of the Surf Day concept, this time targeting deceptive UCE messages. Commission staff conducted a "fall harvest" by surfing the Commission's large database of UCE solicitations, topic by topic, and identifying over 1000 individuals or companies potentially responsible for misleading e-mail solicitations, for example, for pyramid or other get-rich-quick schemes. Ironically, most of these UCE messages did not allow any reply by e-mail, due to inaccurate or deceptive "sender" information, so in January through the U.S. Postal system the Commission sent out letters warning the sources of the UCE that their messages may be in violation of the law.

Our messages to businesses on the Internet are straightforward -- *e.g.*, don't lie or make misleading statements; don't make product or earnings claims that you can't support; don't mislead consumers with unrealistic testimonials. The difficulty lies in finding a way to get these basic messages to new entrepreneurs who may have no prior business or advertising experience. Surf Days help us overcome this hurdle, but in addition, we have put together a "road show" that our ten regional offices can use in their local communities to help explain how basic legal principles apply on the Internet. The Commission also is preparing a business guide for Internet entrepreneurs and a continuing legal education ("CLE") course for lawyers who counsel new Internet businesses. Finally, the Commission is going directly to the computer industry for help. In July, Commission representatives met with Silicon Valley executives at Stanford University's Technology and Business Strategy Summit '97, and asked them to lend us their contacts and marketing expertise in order to reach new Internet entrepreneurs.

Looking Ahead

Currently, the Commission receives approximately 100 to 200 Internet-related complaints per month. Many of these complaints are forwarded to us by the National Fraud Information Center, with which the Commission works closely. The Commission has seen an increase in complaints over the last year, but fortunately on-line problems seem to be growing at a slower pace than the Internet marketplace itself. At the moment, complaints about Internet fraud remain a small fraction of the number of complaints the Commission receives about more traditional problems concerning credit cards or telemarketing. However, the Commission expects that as the Internet marketplace grows, reports about consumer fraud also will continue to grow.

The potential for fraud is likely to be fueled by easy on-line access that exists for legitimate and fraudulent businesses alike. Also, it is likely that many first-time entrepreneurs, because of their lack of marketing experience or knowledge of their

obligations under basic consumer protection principles, will unwittingly engage in Internet practices that violate the law. Finally, keeping up with the introduction and application of new technologies will prove daunting. The growing problem of "spam" already threatens to outstrip our resources. The Commission currently receives approximately 500 pieces of UCE per day, forwarded by disgruntled consumers and others -- far more than we can read or analyze on an individual basis and a volume that strains the capacity of the agency's computers.

To combat on-line fraud, the Commission will continue to use the Internet itself as a tool to improve and enhance our investigations. The Commission's staff all have Internet access, and scores of attorneys, paralegals, and investigators in our Bureau of Consumer Protection have received intermediate or advanced training on use of the Internet to combat fraud.[(28)]

Looking into the future, we anticipate that traditional types of deception -- including pyramid schemes, bogus business opportunities, and failures to deliver promised goods or services -- will continue to top our list of Internet problems. The Commission will continue to be vigilant in monitoring the Internet for new schemes that ingeniously exploit the new technology, like the "Trojan horse" software scheme challenged in the *Audiotex Connection* case. Fighting fraud over the Internet is clearly a formidable task for the FTC's limited available resources. The Commission will do all it can, however, to curb this threat to the continued growth of the Internet and the benefits the Internet can bring consumers through speed, efficiency, convenience, and information never before available.

Conclusion

The Commission recognizes that we stand at a critical juncture in the development of electronic commerce. Although we have seen an explosion in on-line shopping and advertising, fraud and deception may deter consumers from acquiring a greater confidence in the Internet as a place to transact business. The Commission will continue its efforts to fight fraud and deception on line by implementing a comprehensive strategy that combines traditional law enforcement with aggressive consumer and business education.

---

1. My oral testimony and responses to questions you may have reflect my own views and are not necessarily the views of the Commission or any other Commissioner.

2. 15 U.S.C. § 45(a). The Commission also has responsibilities under approximately thirty additional statutes, *e.g.*, the Clayton Act, 15 U.S.C. § 12, which prohibits various anticompetitive practices; the Truth in Lending Act, 15 U.S.C. §§ 1601 *et seq.*, which mandates disclosures of credit terms; the Fair Credit Billing Act, 15 U.S.C. § 1666 *et seq.*, which provides for the correction of billing errors on credit accounts; and the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*, which establishes rights with respect to consumer credit reports. The Commission also enforces over 35 rules governing specific industries and practices, *e.g.* the Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of

information to prospective franchisees; and the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices.

3. Certain entities, such as banks, savings and loan associations, and common carriers, as well as the business of insurance are wholly or partially exempt from Commission jurisdiction. *See* Section 5(a)(2) of the FTC Act, 15 U.S.C. § 45(a)(2) and the McCarran-Ferguson Act, 15 U.S.C. § 1012(b).

4. The FTC and the FCC promulgated their regulations pursuant to the Telephone Disclosure and Dispute Resolution Act, 15 U.S.C. §§ 5701 *et seq.* The FTC's regulations are at 16 C.F.R. Part 308; the FCC's regulations are at 47 C.F.R. § 64.1501 *et seq.*

5. International Data Corporation, *Dramatic Growth of Web Commerce - From 2.6 Billion in 1996 to more than $220 Billion in 2001* (Aug. 26, 1997) (reported at http://www.idc.com/f/HNR/ic2001f.htm).

6. CommerceNet and Nielsen Media Research, *CommerceNet/Nielsen Media Demographic and Electronic Commerce Study*, Spring '97 (March 12, 1997) (defining adults as individuals over 16 years old) (reported at http://www.commerce.net/work/pilot/nielsen_96/ press_97.html) [hereafter *CommerceNet/Nielsen Demographic Study*, Spring '97]; IntelliQuest Communications, Inc., *Worldwide Internet/Online Tracking Service (WWITS ™): Second Quarter 1997 Study* (Sept. 4, 1997) (reported at http://www.intelliquest.com/about/release32.htm).

7. *CommerceNet/Nielsen Demographic Study*, Spring '97.

8. CommerceNet and Nielsen Media Research, *CommerceNet/Nielsen Media Demographic and Electronic Commerce Study*, Fall '97 (December 11, 1997) (reported at http://www.commerce.net/news/press/121197.html) [hereafter *CommerceNet/Nielsen Demographic Study*, Fall '97]. *See also*, Yankelovich Partners, *1997 Cybercitizen Report* (Mar. 27, 1997) (reported at http://www.yankelovich.com/pr/970327.HTM) (finding that 23% of users ordered and paid for a product over the Internet, *i.e*. "transacted" business online).

9. Jupiter Communications, *1998 Online Advertising Report* (Aug. 22, 1997) (reported at http://www.jup.com/digest/082297/advert.shtml) (figure includes directory listings and classified advertisements).

10. *See* Exhibit 1, Bureau of Consumer Protection, Federal Trade Commission, *Anticipating the 21st Century: Consumer Protection in the New High-Tech, Global Marketplace,* iii (May 1996).

11. 15 U.S.C. § 45.

12. 15 U.S.C. § 53(b). In addition, the Commission may request the Attorney General to file an action in the appropriate federal district court seeking civil penalties for violations of the Commission's administrative orders or trade regulation rules, and may file those actions on its own behalf if the Department of Justice declines to do so in the name of the United States. 15 U.S.C. § 56.

13. *America Online, Inc.*, FTC File No. 952-3331 (consent order subject to final approval, May 1, 1997); *CompuServ, Inc.*, FTC File No. 962-3096 (consent order subject to final approval, May 1, 1997); *Prodigy Services Corp*., FTC File No. 952-3332 (consent order subject to final approval, May 1, 1997). These respondents allegedly made "free trial" offers to consumers without adequately disclosing that consumers would automatically be charged if they did not affirmatively cancel before the end of the trial period. (The Commission also alleged that AOL failed to inform consumers that 15 seconds of connect time was added to each online session, resulting in additional undisclosed charges, and that AOL misrepresented that it would debit customers' bank accounts only after receiving authorization to do so.)

14. *E.g.*, **Alleged credit repair scams:** *FTC v. Corzine*, No. CIV-S-94-1446 (E.D. Cal. filed Sept. 12, 1994); *FTC v. Consumer Credit Advocates,* No. 96 Civ. 1990 (S.D.N.Y., filed Mar. 19, 1996);*Martha Clark, d/b/a Simplex Services,* Docket No. C-3667 (consent order, June 10, 1996); *Bryan Coryat, d/b/a Enterprising Solution,*. Docket No. C-3666 (consent order, June 10, 1996); *Lyle R. Larson, d/b/a Momentum,* Docket No. C-3672 (consent order, June 12, 1996); *Rick A. Rehem, d/b/a NBC Credit Resource Publishing,* Docket No. C-3671 (consent order, June 12, 1996). **Alleged business opportunity scams**: *FTC v. Intellicom Services, Inc.,* No. 97-4572 TJH (Mcx)(C.D. Cal., filed June 23, 1997); *FTC v. Chappie (Infinity Multimedia),* No. 96-6671-CIV- Gonzalez (S.D. Fla., filed June 24, 1996); *Timothy R. Bean, d/b/a D.C. Publishing Group,* Docket No. C-3665 (consent order, June 10, 1996); *Robert Surveys, d/b/a Excel Communications,* Docket No. C-3669 (consent order, June 12, 1996); *Sherman G. Smith, d/b/a Starr Communications,* Docket No. C-3668 (consent order, June 12, 1996). **Alleged deceptive cash grant matching service**: *Randolf D. Alberton, d/b/a Wolverine Capital*, Docket No. C-3670 (consent order, June 12, 1996). **Alleged deceptive advertising of health product:** *Global World Media Corp. and Sean Shayan,* Docket No. C-3772 (consent order, Oct. 9, 1997). **Alleged misrepresentations about product characteristics:** *Zygon International, Inc.*, Docket No. C-3686 (consent order, Sept. 24, 1996). **Alleged non-delivery of ordered merchandise:** *FTC v. Brandzel,* 96 C. 1440 (N.D. Ill., filed Mar. 13, 1996).

15. *E.g., FTC v. The Mentor Network, Inc.*, Civ. No. SACV96-1104 LHM (EEx) (C.D. Cal., filed Nov. 5, 1996); *FTC v. Global Assistance Network for Charities,* Civ. No. 96-02494 PHX RCB (D. Ariz., filed Nov. 5, 1996); *FTC v. JewelWay International, Inc*., CV97-383 TUC JMR (D. Ariz., filed June 24, 1997); *FTC v. Rocky Mountain International Silver and Gold, Inc*., Action No. 97-WY-1296 (D. Colo., filed June 23, 1997).

16. Civ. No. C96-799M (W.D. Wash., filed May 23, 1996).

17. *FTC v. Nia Cano d/b/a Credit Development Int'l & Drivers Seat Network*, No. 97-7947 IH (AJWx) (C.D. Cal. filed Oct. 29, 1997).

18. In addition, UCE often contains fake or altered routing information in the address portion of a message, *i.e.*, the "From," "Received from," or "Reply to" lines. Thus, consumers may not know who sent the e-mail or to whom they should reply. Fake "Reply to" lines also may send undeliverable or reply messages back to the wrong address, thereby tying up a legitimate business's computer. This may confuse consumers, but in addition, UCE may directly deceive them through misleading advertisements or solicitations that appear in the body of the e-mail itself. The Commission has received, directly or by referral from consumers, over 50,000 UCE messages. Our staff actively reviews these messages and investigates purveyors of UCE that may violate the FTC Act's prohibition against unfair or deceptive practices.

19. The Commission would like to acknowledge the assistance of AT&T and MCI in administering the redress program. AT&T and MCI will distribute refunds to most consumers in the form of telephone credits on their long-distance telephone bills.

20. A "hit" occurs when someone accesses a web site.

21. After the home page for FTC.GOV, the search engine is the most popular area visited on the web site, followed by the ConsumerLine section. *See* Exhibit 2, excerpts from "www.ftc.gov".

22. Exhibit 3, homepage of "www.consumer.gov".

23. To alleviate any privacy concerns that consumers may have, the warning page makes it clear that the FTC has not gathered any personal information about individuals visiting this teaser site.

24. Exhibit 4, examples of FTC teaser sites.

25. Exhibit 5, example of FTC teaser site highlighted as "new" site of the week by Yahoo!, a large Internet search engine and indexing service.

26. Apart from newsgroup messages that had terminated automatically, 66 (18%) of the notified web sites had been improved or taken down within a month. In the wake of a subsequent Surf Day that targeted a separate type of fraud, 24% of the notified web sites improved or removed their solicitations.

27. International participants included Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Hungary, Ireland, Jamaica, Japan, Korea, Mexico, New Zealand, Norway, the Philippines, Poland, Portugal, South Africa, Spain, Sweden, Switzerland, and the United Kingdom.

28. The Bureau of Consumer Protection's internal Internet Training Committee provided comprehensive one or two-day Internet training sessions in both 1996 and 1997. Not only did Commission employees attend, but also officials from the FBI, the Department of Justice, U.S. Attorney's Offices, as well as state representatives from the National Association of Attorneys General. The training covered legal issues, on-line fraud, emerging technologies, and investigational techniques.