

**PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION ON
"INTERNET FRAUD"**

**Before the
COMMITTEE ON FINANCE
UNITED STATES SENATE
Washington, D.C.
April 5, 2001**

Mr. Chairman, I am Hugh Stevenson, Associate Director of the Division of Planning and Information in the Federal Trade Commission's Bureau of Consumer Protection. I am pleased to be here today to testify about the FTC's efforts to combat fraud on the Internet.⁽¹⁾

As one of the transforming events of our time, the advent of the Internet already has had a profound impact on the marketplace. The Internet has the potential to deliver goods and services more conveniently, faster, and at lower prices than traditional marketing methods. Moreover, at an ever increasing rate, it is stimulating the development of innovative products and services barely conceivable just a few years ago, and enabling consumers to tap into rich sources of information that they can use to make better-informed purchasing decisions.

These developments promise enormous benefits to consumers and the economy. There is real danger, however, that these benefits may not be fully realized if consumers identify the Internet with fraud operators. Fraud on the Internet is an enormous concern for the Commission, and it has prompted a vigorous response using all the tools at the Commission's disposal, including law enforcement and education. The Commission appreciates the Subcommittee's interest in our Internet fraud program, and the Congress' support for funding both the development of our fraud database, Consumer Sentinel, and the creation of our toll-free consumer helpline. The Commission welcomes this opportunity to describe its Internet program and the challenges the agency is confronting.

I. Introduction and Background

A. The FTC and its Law Enforcement Authority

The FTC is the federal government's primary consumer protection agency. While most 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 against "unfair or deceptive acts or practices" and to promote vigorous competition in the marketplace. The FTC Act authorizes the Commission to halt deception through civil actions filed by its own attorneys in federal district court, as well as through administrative cease and desist actions.⁽⁴⁾ Typically these civil actions seek preliminary

and permanent injunctions to halt the targeted illegal activity, as well as redress for injured consumers. Where redress is impracticable, Commission actions generally seek disgorgement to the U.S. Treasury of defendants' ill-gotten gains. As discussed below, these tools have proven to be effective in fighting a broad array of fraudulent schemes on the Internet, in spite of the sheer size and reach of the Internet.

B. The Growth of Ecommerce and Internet Fraud.

The growth of the Internet and ecommerce has been explosive. The number of American adults with Internet access grew from about 88 million in mid-2000 to more than 104 million at the end of the year.⁽⁵⁾ Just this past holiday season, consumers spent an estimated \$10.8 billion shopping on the Internet -- a greater than 50 percent increase over the \$7 billion they spent online during the same period in 1999.⁽⁶⁾ Total ecommerce sales for 2000 were an estimated \$25.8 billion, .8 percent of all sales.⁽⁷⁾

Unfortunately, but not surprisingly, the boom in ecommerce has opened up fertile ground for fraud. The Commission's experience is that fraud operators are always among the first to appreciate the potential of a new technology to exploit and deceive consumers. Long-distance telemarketing attracted con artists when it was introduced in the 1970's. They swarmed to pay-per-call technology when it became available in the late 1980's. Internet technology is the latest draw for opportunistic predators who specialize in fraud. The rapid rise in the number of consumer complaints related to online fraud and deception bears this out: in 1997, the Commission received fewer than 1,000 Internet fraud complaints through Consumer Sentinel; a year later, the number had increased eight-fold. In 2000, over 25,000 complaints -- roughly 26 percent of all fraud complaints logged into Consumer Sentinel by various organizations that year -- related to online fraud and deception. The need -- and challenge -- is to act quickly to stem this trend while the online marketplace is still young.

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 170 Internet-related cases against over 573 defendants. It obtained injunctions stopping the illegal schemes, and ordering more than \$180 million in redress or disgorgement,⁽⁸⁾ and obtained orders freezing millions more in cases that are still in litigation. Its federal district court actions alone have stopped consumer injury from Internet schemes with estimated annual sales of over \$250 million.⁽⁹⁾

II. Challenges Posed by Internet Fraud

The Commission faces a host of novel challenges in its efforts to combat fraud and deception online. Because it is both global in its reach and instantaneous, the Internet lends itself well not only to adaptations of traditional scams - such as pyramid schemes and false product claims - but also to new high-tech scams that were not possible before

development of the Internet. In addition, the Internet enables con artists to cloak themselves in anonymity, which makes it necessary for law enforcement authorities to act much more quickly to stop newly-emerging deceptive schemes before the perpetrators disappear. And because the Internet transcends national boundaries, law enforcement authorities must be more creative and cooperative to successfully combat online fraud. These novel challenges are discussed in greater detail below.

A. Combating Internet Fraud Requires New Methods of Collecting and Analyzing Information.

The Commission is developing new methods of collecting and analyzing information about both the offline and online marketplace, drawing upon the power of new technology itself. A central part of this effort is Consumer Sentinel, a web-based consumer fraud database and law enforcement investigative tool.⁽¹⁰⁾ Consumer Sentinel receives Internet fraud complaints from the FTC's Consumer Response Center ("CRC"), which processes both telephone and mail inquiries and complaints.⁽¹¹⁾ For those consumers who prefer the online environment, an electronic complaint form at www.ftc.gov, first available in May of 1998, permits consumers to channel information about potential scams directly to the CRC and the fraud database.

Consumer Sentinel also benefits from the contributions of many public and private partners. It receives data from other public and private consumer organizations, including 64 local offices of the Better Business Bureaus across the nation, the National Consumers League's National Fraud Information Center, and Project Phonebusters in Canada. Additionally, a U.S. Postal Inspector has served for the past year as the program manager, and the U.S. Postal Inspection Service just signed an agreement to begin sharing 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, the 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, local 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.⁽¹²⁾

The central role that Consumer Sentinel plays in the Commission's law enforcement is exemplified by "Operation Top Ten Dot Cons," the Commission's latest broad "sweep" of fraudulent and deceptive Internet scams. In a year-long law enforcement effort, the FTC and four other U.S. federal agencies,⁽¹³⁾ consumer protection organizations from 9 countries,⁽¹⁴⁾ and 23 states⁽¹⁵⁾ announced 251 law enforcement actions against online scammers. The FTC brought 54 of the cases.⁽¹⁶⁾ The top 10 scams, identified through analysis of complaint data in the Consumer Sentinel database, were:

- Internet Auction Fraud
- Internet Service Provider Scams
- Internet Web Site Design/Promotions ("Web Cramming")⁽¹⁷⁾
- Internet Information and Adult Services (unauthorized credit card charges)
- Pyramid Scams
- Business Opportunities and Work-At-Home Scams
- Investment Schemes and Get-Rich-Quick Scams
- Travel/Vacation Fraud
- Telephone/Pay-Per-Call Solicitation Frauds (including modem dialers and videotext)⁽¹⁸⁾
- Health Care Frauds

The Consumer Sentinel data enabled the FTC and the other enforcement agencies that joined us in this project both in the U.S. and abroad to identify not only the top ten types of scams, but also the specific companies generating the highest levels of complaints about each of those types of scams. These companies became the targets for the law enforcement actions that comprised Operation Top Ten Dot Con. Finally, Consumer Sentinel data enabled the Commission and its partners to obtain and develop evidence against these targets from individual consumers whose complaints had been included in the database.

Consumer Sentinel first went online in late 1997. Since then, the Commission has upgraded the capacity of the Consumer Sentinel database and enhanced the agency's complaint-handling systems by creating and staffing a new toll-free consumer helpline at 1-877-FTC-HELP, and adding several new functions to Consumer Sentinel. The first of these new functions, the "Top Violators" report function, allows a law enforcement officer to pull up the most common suspects and schemes by state, region or subject area. The second new function, "Auto Query," enables an investigator to create an automatic search request. This automatic search can be set to run daily, weekly or monthly, and if new complaints come in to Consumer Sentinel that match the search criteria, Consumer Sentinel will automatically alert the investigator via email. Third, the "Alert" function enables law enforcers to communicate with each other and minimize duplication of their efforts, and a fourth new function performs a search of Commission court orders online. In 2000, Consumer Sentinel received over approximately 100,000 consumer complaints.⁽¹⁹⁾ Currently the database holds over 300,000 consumer complaints.⁽²⁰⁾

The Commission's efforts to improve consumer complaint collection and analysis

through the Consumer Response Center and Consumer Sentinel are complemented by a proactive program to uncover fraud and deception in broad sectors of the online marketplace through "Surf Days." Surf Days use new technology to detect and analyze emerging Internet problems. While Consumer Sentinel provides data on broad trends and the volume of complaints prompted by particular Internet schemes, Surf Days allow the Commission to take a "snap shot" of a market segment at any given time. The Commission also uses Surf Days to reach new entrepreneurs and alert those who unwittingly may be violating the law.

On a typical Surf Day, Commission staff and personnel from our law enforcement partners -- often state attorneys general, sister federal agencies or private organizations like the Better Business Bureau -- widely "surf" the Internet for a specific type of claim or solicitation that is likely to violate the law. When a suspect site is identified, the page is downloaded and saved as potential evidence, and the operator of the site is sent an email warning that explains the law and provides a link to educational information available at www.ftc.gov. Shortly thereafter, a law enforcement team revisits the previously warned sites to determine whether they have remedied their questionable claims or solicitations. The results vary, depending on the targeted practice of the particular Surf Day. In each of these efforts, between 20 to 70 percent of the Web site operators who received a warning come into compliance with the law, either by taking down their sites or modifying their claims or solicitations. Sites that continue to make unlawful claims are targeted for possible law enforcement action.

To date, the Commission has conducted 26 different Surf Days targeting problems ranging from "cure-all" health claims to fraudulent business opportunities and credit repair scams.⁽²¹⁾

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 proven so 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 schemes, 25 cases against deceptive business opportunities and work-at-home scheme, and 11 cases against pyramid schemes.

It is no surprise that the Internet versions of traditional frauds can be much larger in size and scope than their offline predecessors. A colorful, well-designed Web site imparts a sleek new veneer to an otherwise stale fraud; and the reach of the Internet allows an old-time con artist to think -- and act -- globally, as well.

Pyramid schemes are the most notable example of a fraud whose size and scope are magnified by the Internet.⁽²²⁾ By definition, these schemes require a steady supply of new recruits. The Internet provides an efficient way to reach countless new prospects around the world, and to funnel funds more efficiently and quickly from the victims to the scammers at the top of the pyramid. As a result, the victims are more numerous, the fraud operator's financial "take" is much greater, and the defense is typically well-funded and fierce when the FTC brings suit to stop a pyramid scheme operating online.

Despite the extensive resources required to pursue an online pyramid case, the Commission has asserted a strong enforcement presence, obtaining orders to pay more than \$70 million in redress for victims,⁽²³⁾ and pursuing millions more in ongoing litigation. In one case, *FTC v. Fortuna Alliance*, the Commission spent two years in litigation and negotiations and finally obtained a court order finding the defendants in contempt, and a stipulated final order enjoining the defendants from further pyramid activities and requiring them to pay \$5.5 million in refunds to over 15,000 victims in the U.S. and 70 foreign countries.⁽²⁴⁾ More recently, in *FTC v. Five Star Auto Club, Inc.*,⁽²⁵⁾ the Commission prevailed at trial against another pyramid scheme that lured online consumers to buy in by claiming that an annual fee and \$100 monthly payments would give investors the opportunity to lease their "dream vehicle" for "free" while earning between \$180 and \$80,000 a month by recruiting others to join the scheme. The court issued a permanent injunction shutting down the scheme, barring for life the scheme's principals from any multi-level marketing business, and ordering them to pay \$2.9 million in consumer redress.

C. Scams Are Increasingly High-Tech.

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 with -- 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-tech fraud, the Commission has supported staff training and given its staff the tools to be effective cyber-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 held 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 including 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-tech fraud. The FTC's Internet Lab is an important example. With high speed computers that are separate from the agency's network and loaded with the latest hardware and software, the Lab allows staff to investigate fraud and deception in a secure environment and to preserve evidence for litigation.

The Commission has used its training and tools to stop some of the most egregious and technically sophisticated schemes seen on the Internet. For example, the FTC's lawsuit against Verity International, Ltd.,⁽²⁶⁾ was prompted by the influx of hundreds of complaints in the last week of September 2000 through the CRC and logged in Consumer Sentinel. Investigation showed that high charges on consumers' phone lines were being initiated by "dialer" software downloaded from teaser adult web sites. Many line subscribers had no idea why they received bills for these charges. Others discovered that a minor in their household -- or another person who did not have the line subscriber's authorization -- accessed the Web sites and downloaded the dialer software. The dialer program allowed users to access the "videotext" adult content without any means of verifying that the user was the line subscriber, or was authorized by the line subscriber to 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 reconnecting the consumer's modem to the Internet from some overseas location, opening at an adult web site. The line subscriber -- the consumer responsible to pay phone charges on the telephone line -- then began incurring charges on their 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.⁽²⁷⁾

Earlier, in *FTC v. Carlos Pereira d/b/a atariz.com*,⁽²⁸⁾ 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 some one else'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 25 million 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 subjects as innocuous as "Oklahoma tornadoes" or "child car seats" would type those terms into a search engine and the search results would list a variety of related sites, including the bogus, copycat site of the defendants. Surfers assumed from the listings that the defendants' sites contained the information they were seeking and clicked on the listing. The "redirect" command imbedded in the copycat site immediately rerouted the consumer to an adult site hosted by the defendants. Once there, defendants "mousetrapped" consumers by incapacitating their Internet browser's "back" and "close" buttons, so that while they were trying to exit the defendants' site, they were sent to

additional adult sites in an unavoidable, seemingly endless loop.

Using the new tools available in the Internet Lab, the Commission was able to capture and evaluate evidence of this "pagejacking" and "mousetrapping." In September 1999, the Commission filed suit in federal court and obtained a preliminary order stopping these activities and suspending the Internet domain names of the defendants. Since then, the Court has entered default judgments against two defendants and a stipulated permanent injunction against a third, barring them from future law violations. A fourth defendant, Carlos Pereira, has evaded law enforcement authorities in Portugal.

D. 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, short-lived Web sites, and falsified domain name registrations, many fraud operators are able to strike quickly, victimize thousands of consumers in a short period of time, and disappear nearly without a 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 problems, conduct quick but thorough investigations, and prepare cases for filing in federal courts. Based on such data review, FTC staff had completed the investigation and was in court successfully arguing for an *ex parte* temporary restraining order and asset freeze in *FTC v. Verity International, Ltd.* within a little more than a week after the first complaints begin coming in to the Consumer Response Center.

In another exemplary effort of the Rapid Response Team, *FTC v. Benoit*,⁽³⁰⁾ the Team quickly moved against defendants who allegedly used deceptive emails or "spam" to dupe consumers into placing expensive international audiotext calls.⁽³¹⁾ 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. Most 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.

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 in 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.

E. 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 company executives, business representatives, legal scholars, consumer advocates, and state and federal officials presented testimony, and the Commission published a two-volume report summarizing the testimony and the role of antitrust and consumer protection law in the 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.⁽³²⁾ 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 ecommerce 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 off-shore. For example, in *FTC v. J.K. Publications*,⁽³³⁾ the Commission obtained an *ex parte* temporary restraining order, a preliminary injunction and an asset freeze against defendants that allegedly made unauthorized charges of \$19.95 per month on consumers' credit or debit cards for purported Internet services. Based upon evidence gathered by Commission staff, the defendants may have charged over 900,000 consumers a total of \$45 million for unordered or unauthorized Internet services. According to the receiver appointed in this case, the defendants moved millions of dollars to the Cayman Islands, Liechtenstein, and Vanuatu in the South Pacific. The Commission continues to litigate this case, and the receiver continues to attempt to locate defendants' foreign assets and repatriate them to the U.S.

In *FTC v. Fortuna Alliance*, one of the pyramid schemes described above, 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 final judgment in U.S. court that required the defendants to repatriate that money for consumer redress. In the process, however, it cost \$280,000 in fees alone to litigate the case in foreign court.⁽³⁴⁾

In addition to fraud proceeds moving off-shore quickly, fraudulent online operators may be beyond the reach of the Commission and U.S. courts, practically if not legally. There is now 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 remedies available under U.S. law and must work more cooperatively with law enforcement officials in other countries. To that end, the FTC has executed cooperation memoranda with

agencies in Canada, the United Kingdom, and Australia.⁽³⁵⁾

The Commission's actions in *FTC v. Pereira* represent significant strides in the right direction. In that case, the Commission realized that the defendants' "pagejacking" and "mousetrapping" scheme had operated through Web sites registered with a U.S.-based company. Thus, in its request for a temporary restraining order and preliminary injunction, the Commission asked that the registrations for these Web sites be suspended, thereby effectively removing the defendants and their deceptive Web sites from the Internet, pending a full trial. At the same time, the Commission reached out to its international colleagues in Portugal and Australia. The Australian Competition and Consumer Commission (ACCC) proved especially helpful in providing information about the defendants and their business operations in Australia. The ACCC also began its own investigation, executed a number of search warrants, and began pursuing potential legal action against the defendants in that country.

III. Consumer and Business Education

Law enforcement alone cannot stop the tide of fraudulent activity on the Internet. Meaningful consumer protection depends on education as well. Consumers must be given the tools they need to spot potentially fraudulent promotions, and businesses must be advised about how to comply with the law. The FTC's consumer and business education program uses the Internet to communicate anti-fraud and educational messages to reach vast numbers of people in creative and novel ways quickly, simply and at low cost. As more consumers and businesses come online, use of the Internet to disseminate information will grow.

A. Fraud Prevention Information for Consumers

More than 200 of the consumer and business publications produced by the FTC's Bureau of Consumer Protection are available on the agency's Website in both text and .pdf format. Indeed, the growth in the number of our publications viewed online between 1996 and 1999 (140,000 vs. 2.5 million) tells the story of the Internet's coming of age as a mainstream medium and highlights its importance to any large-scale dissemination effort. Those 2.5 million page views are in addition to the 6 million print publications the FTC distributes each year to organizations that disseminate them on the FTC's behalf.

B. Link Program

In addition to placing publications on its own Web site, the FTC actively encourages partners - government agencies, associations, organizations, and corporations with an interest in a particular subject - to link to its information from their sites and to place banner public service announcements provided by the FTC on their sites. Links from the banners allow visitors to click through to the FTC site quickly to get the information they're looking for exactly when they want it. Examples of the varied organizations that have helped drive traffic to the valuable consumer information on www.ftc.gov are Yahoo!, American Express, Circuit City, AARP, North American Securities

Administrators Association, the Alliance for Investor Education, the Better Business Bureau, CBS, motleyfool.com, the U.S. Patent and Trademark Office, Shape Up America!, the National Institutes of Health, and the Arthritis Foundation.

C. "Teaser" Pages

Too often, warning information about frauds reaches consumers after they've been scammed. For the FTC, the challenge is reaching consumers before they fall victim to a fraudulent scheme. Knowing that many consumers use the Internet to shop for information, agency staff have developed teaser sites that mimic the characteristics that make a site fraudulent and then warn the reader about the fraud. Metatags embedded in the FTC teaser sites make them instantly accessible to consumers who are using major search engines and indexing services as they look for products, services and business opportunities online. The teaser pages link back to the FTC's page, where consumers can find practical, plain English information. The agency has developed more than a dozen such teaser sites on topics ranging from fraudulent business opportunities and wealth-building scams to weight loss products, vacation deals and investments.⁽³⁶⁾ Feedback from the public has been overwhelmingly positive: visitors express appreciation -- not only for the information, but for the novel, hassle-free and anonymous way it is offered.

D. Consumer.gov.

Following its vision of the Internet as a powerful tool for consumer education and empowerment, the FTC organized a group of five small federal agencies in 1997 to develop and launch a Web site that would offer one-stop access to the incredible array of federal consumer information. On the theory that consumers may not know one federal agency from another, the information is arranged by topic area. Federal agencies have responded well to consumer.gov. The site now includes contributions from 170 federal agencies. Consumers also find it useful, with over 182,500 visits to the site recorded in the first half of FY 2001.

Visitors to consumer.gov find special initiatives, too: The President's Council on Y2K Conversion asked the FTC to establish a Y2K consumer information site; the Quality Interagency Coordination Task Force requested a special site on health care quality; and the U.S. Postal Inspection Service asked that consumer.gov house the site to support the **kNOW Fraud** initiative, an ongoing public-private campaign initiated with the sending of postcards about telemarketing fraud to 115 million American households in the fall of 1999.⁽³⁷⁾ The FTC continues to maintain the site.

E. Business Education for Online Marketers

As part of its mission, the FTC provides guidance to online marketers on how to assure that basic consumer protection principles apply online. Many of these entrepreneurs are small, start-up 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.⁽³⁸⁾ FTC also has used a variety of other approaches to get its messages out to the business community, from posting compliance guides, staff advisory letters and banner public service announcements on the Web to speaking at industry and academic meetings and conferences, using the trade press to promote the availability of information on the agency site, and holding workshops on online issues and posting the transcripts. Most recently, on January 30 of this year, the Commission, in cooperation with the Electronic Retailing Association presented "Etail Details" a case-driven Internet marketing seminar for Internet retailers, marketers, and suppliers on applying offline rules and regulations online. The seminar was designed to ensure etailers understand and comply with FTC rules regarding etailing.

IV. Conclusion

The Commission has been involved in policing the electronic marketplace for six years - before the World Wide Web was widely used by consumers and businesses. So far, we have kept pace with the unprecedented growth of the electronic marketplace by targeting our efforts, making innovative use of the technology, and leveraging our resources. We have done all this with limited resources, and 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.

-
1. The views expressed in this statement represent the views of the Commission. My responses to any questions you may have are my own and are 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 banks, savings associations, and federal credit unions; regulated common carriers; air carriers; non-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. § 21 (Clayton Act); 7 U.S.C. § 227 (Packers and Stockyards Act); 15 U.S.C. § 1011 *et seq.* (McCarran-Ferguson Act).
 3. 15 U.S.C. § 45(a). The Commission also has responsibilities under more than 45 additional statutes, *e.g.*, 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.*, which mandates disclosures of credit terms; and the Fair Credit Billing Act, 15 U.S.C. §§ 1666 *et. seq.*, which provides for the correction of billing errors on credit accounts. 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.
 4. 15 U.S.C. §§ 45(a) and 53(b).
 5. Pew Internet and American Life Project, *More Online, Doing More* (reported at

<http://www.pewinternet.org/reports/toc.asp?Report=30>) (stating that comparing figures gathered in tracking survey in May and June with figures gathered between Thanksgiving and Christmas, the number of American adults with Internet access grew from about 88 million to more than 104 million in the second half of 2000).

6. Jupiter Communications, Inc., *Online Holiday Sales Increased by 54 percent this Holiday Season, Despite Dot Com Closures and Soft Offline Purchase* (Jan. 17, 2001) (estimating Nov. and Dec. 2000 online sales of \$10.8 billion, compared to \$7 billion for those months in 1998) (reported at www.jup.com/company/pressrelease.jsp?doc=pr010117). The Census Bureau of the Department of Commerce estimated that in the fourth quarter of 2000, not adjusted for seasonal, holiday, and trading-day differences, online retail sales were \$8.686 billion, an increase of 67.1 percent from the 4th quarter of 1999 (reported at www.census.gov/mrts/www/current.html).

7. *Id.*

8. To date the Commission has collected more than \$55 million in redress for victims of Internet fraud and deception.

9. These figures are based on estimated annual fraudulent sales by defendants in the twelve months prior to filing the complaint. Fraudulent sales figures are based on, among other things, financial statements, company records, receiver reports, and deposition testimony of company officials.

10. See www.consumer.gov/sentinel.

11. The CRC now receives over 12,000 inquiries and complaints per week. They cover a broad spectrum -- everything from complaints about get-rich-quick telemarketing scams and online auction fraud, to questions about consumer rights under various credit statutes and requests for educational materials. Counselors record complaint data, provide information to assist consumers in resolving their complaints, and answer their inquiries.

12. In 1998, the Interagency Resources Management Conference Award recognized Consumer Sentinel as an exceptional initiative to improve government service.

13. U.S. agencies participating included the Commodity Futures Trading Commission, the Department of Justice, the Securities and Exchange Commission and the United States Postal Inspection Service.

14. Participants in "Operation Top Ten Dot Cons" included consumer protection agencies from Australia, Canada, Finland, Germany, Ireland, New Zealand, Norway, the United Kingdom and the United States.

15. Cases were brought by the Attorneys General of Arizona, Colorado, Florida, Illinois, Iowa, Indiana, Louisiana, Maryland, Massachusetts, Michigan, Missouri, Nevada, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania, Tennessee, Texas, and Washington State. Consumer protection offices in West Virginia, and Wisconsin also took action, as did the Louisiana Department of Justice, the Oklahoma Department of Securities, and the Washington State Securities Division.

16. The SEC's contribution to this project consisted of 77 cases.

17. "Web cramming" is a type of unauthorized billing scam. Web crammers call their victims--often small businesses--and offer a "free" Web page; then they start billing the victims, typically on their monthly telephone statements, without authorization. In many cases the small business victims are not even aware that they have a web site or are paying for one.

18. Telephone/Pay-Per-Call Solicitation Frauds are schemes that exploit the telephone billing and

collection system to charge consumers for telephone-based entertainment programs ("audiotext" in industry parlance) or other so-called "enhanced services" that are not telecommunications transmission but are often billed on consumers' telephone bills. Modem dialers and videotext schemes, like the operation attacked in *FTC v. Verity International*, No.00 Civ. 7422(LAK) (S.D.N.Y. 2000), described *infra*, are ones that, unbeknownst to a consumer, cause his or her computer modem to disconnect from his or her usual Internet service provider, dial an expensive international telephone number, and reconnect to the Internet at a remote location overseas, charging the consumer as much as \$5.00 or more per minute for as long as the consumer continues online.

19. Consumer Sentinel has also been upgraded and expanded to provide participants access to the Identity Theft Data Clearinghouse, the central repository for federal identity theft complaints

20. The FTC recently has signed an agreement with the Department of Defense to collect consumer complaint from men and women serving in the military through a project called "Soldier Sentinel."

21. The FTC has coordinated or co-sponsored the following Surf Days, listed by date of their announcements: Pyramid Surf Day (Dec. 1996), Credit Repair Surf (April 1997), Business Opportunity Surf Day (April 1997), Coupon Fraud Surf Day (Aug. 1997), North American Health Claims Surf (Oct. 1997), HUD Tracer Surf Day (Nov. 1997), International Surf Day (Oct. 1997), Kids Privacy Surf Day (Dec. 1997), Junk E-mail Harvest (Dec. 1997), Privacy Surf (March 1998), Textile and Wool Labeling Surf (Aug. 1998), Y2K Surf (Sept. 1998), International Health Claims Surf (Nov. 1998), Investment Surf Day (Dec. 1998), Jewelry Guides Surf (Jan. 1999), Pyramid Surf Day II (March 1999), Green Guide Surf (April 1999), Coupon Fraud II Surf Day (June 1999), Jewelry Guides Surf II (January 2000), Scholarship Services Surf (January 2000), GetRichQuick.con Surf (March 2000), False or Unsubstantiated Lice Treatment Claims Surf (April 2000), Credit Repair Surf II (Aug. 2000), Childrens' Online Privacy Protection Act Compliance Surf (Aug. 2000), False Claims of Authenticity for American Indian Arts and Crafts Surf Day (Oct. 2000), and TooLate.Com [Surf of Online Retailers' Compliance with the Mail or Telephone Order Merchandise Rule] (Nov. 2000).

22. Pyramid operators typically promise enormous earnings or investment returns, not based on commissions for retail sales to consumers, but based on commissions for recruiting new pyramid members. Recruitment commissions, of course, are premised on an endless supply of new members. Inevitably, when no more new recruits can be found, these schemes collapse and a vast majority of participants lose the money they invested.

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

24. *FTC v. Fortuna Alliance, L.L.C.*, No. C96-799M (W.D. Wash. 1996). *See also, FTC v. JewelWay International, Inc.*, No. CV97-383 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-990969-JBR-RLH (D.Nev. 1999) (pyramid promoted through many devices, including some use of the Internet; \$50 million in consumer redress).

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

26. *FTC v. Verity International, Ltd.*, No. 00 Civ. 7422 (LAK)(S.D.N.Y. 2000).

27. Other modem hijacking cases include *FTC v. Audiotex Connection, Inc.*, No. CV-97-0726 (DRH) (E.D.N.Y. 1997) (final stipulated injunction halting the unlawful practice and order that 27,000 victims receive full redress totaling \$2.14 million); *FTC v. RJB Telcom, Inc.*, No.CV 00-2017 PHX SRB (D. Az.

2000); *FTC v. Ty Anderson*, No. C 00-1843P (W.D. Wa. 2000).

28. *FTC v. Carlos Pereira d/b/a atariz.com*⁽²⁹⁾

29. Civil Action No. 99-1367-A)

30. *FTC v. Benoit* (previously *FTC v. One or More Unknown Parties*), No. 3:99 CV 181 (W.D.N.C. 1999). In the course of the litigation, Commission attorneys were able to identify the operators of the scheme.

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

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

33. *FTC v. J.K. Publications*, No. 99-000-44ABC (AJWx)(C.D. Cal. 1999).

34. 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.

35. The Commission is increasingly cooperating with international colleagues in a number of venues. Among them is the International Marketing Supervision Network, a group of consumer protection agencies from the 30 countries that are members of the Organization for Economic Cooperation and Development.

36. The titles of the teaser sites are: Looking for Financial Freedom?; The Ultimate Prosperity Page; Nordicalite Weight Loss Product; A+ Fast Ca\$\$h for College; EZTravel: Be an Independent agent; EZTravel: Certificate of Notification; EZToyz Investment Opportunity; HUD Tracer Association; CreditMenders Credit Repair; NetOpportunities: Internet is a Gold Mine; National Business Trainers Seminars; VirilityPlus: Natural Alternative to Viagra; ArthritiCure: Be Pain-Free Forever.

37. The original consumer.gov team received the Hammer Award, presented by the Vice President to teams of federal employees who have made significant contributions to reinventing government.

38. There has been an astonishing growth in page views of this publication in the past year: from 33,448 views in FY 1999 to 110,473 in FY 2000 .