PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION ON

"Unsolicited Commercial E-Mail"

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

Washington, D.C.

November 3, 1999

Mr. Chairman, I am Eileen Harrington of the Federal Trade Commission's Bureau of Consumer Protection. The Federal Trade Commission is pleased to provide testimony today on the subject of unsolicited commercial email, the consumer protection issues raised by its widespread use, and the Federal Trade Commission's program to combat deceptive and fraudulent unsolicited commercial email.[(1)]

I. Introduction and Background

A. FTC Law Enforcement Authority

As the federal government's principal consumer protection agency, the FTC's mission is to promote the efficient functioning of the marketplace by taking action against unfair or deceptive acts or practices, and increasing consumer choice by promoting vigorous competition. To fulfill this mission, the Commission enforces the Federal Trade Commission Act, which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[(2)] The Commission's responsibilities are far-reaching. With certain exceptions, this statute provides the Commission with broad law enforcement authority over virtually every sector of our economy.[(3)] Commerce on the Internet, including unsolicited commercial electronic mail, falls within the scope of this statutory mandate.

B. Concerns about Unsolicited Commercial Email

Unsolicited commercial email -- "UCE," or "spam," in the online vernacular -- is any commercial electronic mail message sent, often in bulk, to a consumer without the consumer's prior request or consent. The staff of the Commission has amassed a database containing over 2 million pieces of UCE. Analysis of this UCE database shows that well-known manufacturers and sellers of consumer goods and services seldom send UCE. Rather, merchants of this type use ***solicited*** email to give consumers information that they have requested about available products, services, and sales. For example, consumers may agree in advance to receive information about

newly-published books on subjects of interest, online catalogues for products or services frequently purchased, or weekly emails about discounted airfares.

These examples of bulk commercial email sent at the consumer's request demonstrate the value of consumer sovereignty to the growth of Internet commerce. Giving consumers the ability to *choose* the information they receive over the Internet -- known in the industry now as "permission-based" marketing -- seems likely to create more confidence in its content and in the sender. Conversely, when unsolicited information arrives in consumers' electronic mailboxes, the consumers who have contacted the Commission have been far less likely to engage in commerce with the sender.

Not all UCE is fraudulent, but fraud operators - often among the first to exploit any technological innovation - have seized on the Internet's capacity to reach literally millions of consumers quickly and at a low cost through UCE. In fact, UCE has become the fraud artist's calling card on the Internet. Much of the spam in the Commission's database contains false information about the sender, misleading subject lines, and extravagant earnings or performance claims about goods and services. These types of claims are the stock in trade of fraudulent schemes.

While bulk UCE burdens Internet service providers and frustrates their customers, the FTC's main concern with UCE is its widespread use to disseminate false and misleading claims about products and services offered for sale on the Internet. The Commission believes the proliferation of deceptive bulk UCE on the Internet poses a threat to consumer confidence in online commerce and thus views the problem of deception as a significant issue in the debate over UCE. Today, Congress, law enforcement and regulatory authorities, industry leaders and consumers are faced with important decisions about the roles of self-regulation, consumer education, law enforcement, and government regulation in dealing with UCE and its impact on the development of electronic commerce on the Internet.

II. The Federal Trade Commission's Approach to Fraud on the Internet

A. Law Enforcement

Deceptive UCE is part of the larger problem of deceptive sales and marketing practices on the Internet. In 1994, the Commission filed its first enforcement action against deception on the Internet, making it the first federal enforcement agency to take such an action.[(4)] Since that time, the Commission has brought over 100 law enforcement actions to halt online deception and fraud. The pace of our Internet law enforcement has been increasing, in step with the growth of commerce -- and fraud -- on the Internet; over half of the FTC's Internet-related actions have been filed since the beginning of this year.

The Commission brings to the Internet a long history of promoting competition and protecting consumers in other once-new marketing media. These past innovations have included television advertising, direct mail marketing, 900-number sales, and telemarketing. The development of each of these advances in the market was marked by early struggles between legitimate merchants and fraud artists as each sought to capitalize on the efficiencies and potential profits of the new way of doing business. In each instance, the Commission used its statutory authority

under Section 5 of the FTC Act to bring tough law enforcement actions to halt specific deceptive or unfair practices, and establish principles for non-deceptive marketing.[5] In some instances, most notably national advertising, industry took an aggressive and strong self-regulatory stance that resulted in dramatic improvements in advertising and marketing practices.[6] In other instances, at the direction of Congress or on its own initiative, the Commission has issued trade regulation rules to establish a bright line between legitimate and deceptive conduct.[7]

B. Monitoring and Studying Industry Practices

The Federal Trade Commission closely monitors the development of commerce on the Internet. Through a series of hearings and public workshops, the Commission has heard the views of a wide range of stakeholders and issued reports on the broad challenges posed by the rapid growth of the Internet and electronic commerce. In the fall of 1995, the Commission held four days of hearings to explore the effect of new technologies on consumers in the global marketplace. Those hearings produced a staff report, *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace*.[8] The report warned of the potential for the Internet to become the newest haven for deception and fraud.

III. The Commission's Approach to Unsolicited Commercial E-Mail

A. Monitoring the Problem

In June 1997, at a workshop addressing issues of privacy on the Internet, the Commission heard discussion of three distinct UCE problems: (1) deception in UCE content; (2) economic and technological burdens on the Internet and delivery networks caused by the large volume of UCE being sent; and (3) costs and frustrations imposed on consumers by their receipt of large amounts of UCE.

The Commission's immediate concern has been with deceptive UCE. The FTC asked industry and advocacy groups that participated in the privacy workshop to focus on the economic and technological burdens caused by UCE and report their recommendations back to the Commission. Under the leadership of the Center for Democracy in Technology, these groups spent a year studying the problem and identifying possible solutions, and in July 1998 issued their "Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial E-Mail"[9] ("Ad-Hoc Report"). The Ad-Hoc Report recommended the pursuit of technologies and public policies that would give more control to consumers over the UCE they received. Specifically, the report:

- urged marketers to give consumers a choice to "opt in" or "opt out" of receiving a UCE solicitation; and

- urged law enforcement to continue to attack fraudulent UCE solicitations, including those with deceptive "header" information.[10]

On another front, the FTC set up a special electronic mailbox reserved for UCE in order to assess, first hand, emerging trends and developments in UCE. With the assistance of Internet

service providers, privacy advocates, and other law enforcers, staff publicized the Commission's UCE mailbox, "uce@ftc.gov," and invited consumers to forward their UCE to it. The UCE mailbox has received more than 2,010,000 forwarded messages to date, including 3,000 to 4,000 new pieces of UCE every day. Staff enters each UCE message into the database; UCE received and entered in the database within the preceding 6 months is searchable. Periodically, staff analyzes the data, identifies trends, and uses its findings to target law enforcement and consumer and business education efforts.

B. Aggressive Law Enforcement

The Commission has responded to fraudulent UCE with a vigorous law enforcement program. To date, the FTC has brought 17 actions, most of them in federal district court, against schemes that employed spam as an integral part of their operation. For example, in May of this year the Commission filed *FTC v. Benoit, et al.*[(11)] This scheme used the ruse of a spam notification about charges purportedly to be billed to consumers' credit card accounts to lure the consumers into calling an expensive international telephone number.[(12)] The initial spam message purported to inform consumers that their "orders had been received and processed" and that their credit card accounts would be billed for charges ranging from $250 to $899. In fact, the consumers had not ordered anything. The spam advised recipients to call a specified telephone number in area code 767 with any questions about the "order" or to speak to a "representative." Many consumers were unaware that area code 767 is in a foreign country -- Dominica, West Indies -- because it was unnecessary to dial 011 or any country code to make the calls.

Consumers who called to prevent charges to their credit cards, expecting to speak to a "representative" about the erroneous "order," were allegedly connected to an adult entertainment "audiotext" service. Later, these consumers received charges on their monthly telephone bills for the international long-distance call to Dominica, West Indies. The defendants shared in the revenue received by a foreign telephone company for the costly international calls. The defendants hid their tracks by using forged headers in the spam they used to make initial contact with consumers.

The Commission's complaint alleged that the defendants induced consumers to incur charges for a costly international audiotext entertainment service by falsely representing that consumers had placed a merchandise order that would be charged on their credit cards, and that consumers who called a specified telephone number -- actually the number for the audiotext entertainment service -- would receive answers to any questions about the order.

The Commission, on October 26, 1999, approved a stipulated final order resolving the charges in the complaint and the settlement is now awaiting approval by the Court. Under the terms of the settlement, the defendants will be enjoined permanently from misrepresenting any material fact in the course of advertising, promoting, offering, or selling of any good or service. More specifically, the settlement will prohibit the defendants from sending or causing to be sent any email (including unsolicited commercial email) that misrepresents the identity of the sender of the email or the subject of the e-mail. The Order thus prohibits the defendants from falsifying information in the "from" and "subject" lines of e-mails, as well as in the text of the message.

Another recent case, this time targeting an alleged pyramid scheme that centered on spam, is *FTC v. Martinelli*.[13] The defendants in that case ran DP Marketing, a Connecticut-based alleged pyramid scheme, elaborately disguised as a work-at-home opportunity. The scheme solicited new recruits through "spam" and through newspaper classified ads across the country. The spam contained messages such as: "National Marketing Company seeks individuals to handle office duties from home. This is a full or part-time position with a salary of $13.50/hr. The position consists of processing applications for credit, loans or employment, as well as online consumer service."

Consumers responded by visiting DP Marketing's Web site or by calling the company. In either case, the defendants informed the consumers that the $13.50 per hour jobs were for processing orders for DP Marketing from the comfort of their own homes. The defendants further told consumers that no experience was necessary, and that for a "registration fee" ranging from $9.95 to $28.72 they would be sent everything they would need to get started, including telephone scripts, product sheets, time sheets and an ID number. What the consumers actually got was a kit instructing them first to place advertisements identical to the ones they had responded to, and then to read the same script to people who responded to their ads. Instead of $13.50 per hour, the money consumers could earn was based on the number of new victims they recruited.

The FTC charged that the defendants misrepresented to consumers that DP Marketing offers jobs at a specified salary; failed to disclose the material fact that they were offering a pyramid work-at-home scheme; and provided the "means and instrumentalities" to others to commit unlawful and deceptive acts. On September 23, 1999, the court granted the Commission's motion to approve a stipulated preliminary injunction prohibiting the defendants from continuing this scheme.

The Commission has also brought a number of cases against credit repair scams that used spam as an integral aspect of their deception.[14] In a particularly pernicious variation on this scheme, consumers are urged to create a new credit identity in order to fix their credit. Using spam messages such as "BRAND NEW CREDIT FILE IN 30 DAYS," these scammers induce consumers to purchase instructions about how consumers can obtain federally-issued, nine-digit employee identification numbers or taxpayer identification numbers, substitute them for social security numbers, and use them illegally to build new credit profiles that will allow them to get credit they may be denied based on their real credit histories. In fact, using a false identification number to apply for credit is a felony - a point these scammers omit from their solicitations. The Commission, either on its own or through the Department of Justice, filed cases against seven operations that used this type of deceptive spam.[15]

Other types of deceptive schemes that use UCE have also been targets of FTC enforcement action, such as allegedly deceptive business opportunities[16] and deceptive weight loss schemes.[17] As these cases illustrate, the Commission's focus has been on deceptive UCE.

C. Comprehensive Consumer and Business Education

The Commission has published three consumer publications related to UCE. ***Trouble @ the In-Box*** identifies some of the scams showing up in electronic in-boxes. It offers tips and

suggestions for assessing whether an opportunity is legitimate or fraudulent, and steers consumers to additional resource materials that can help them determine the validity of a promotion or money making venture. To date, nearly 62,000 copies of the brochure have been distributed, and it has been accessed on the FTC's web site nearly 19,000 times.

How to Be Web Ready is a reader's bookmark that offers consumers tips for safe Internet browsing. It provides guidance for consumers on how to safeguard personal information, question unsolicited product or performance claims, exercise caution when giving their email address, guard the security of financial transactions, and protect themselves from programs and files that could destroy their hard drives. A number of corporations and organizations have provided a link from their web site to the tips on the FTC's web site, including Circuit City, Borders Group Inc., Netcom, Micron, and Compaq. More than 52,000 copies of the bookmark have been distributed, and it has been accessed more than 15,000 times on the FTC's web site.

In July 1998, the FTC launched a public education campaign called "***Spam's Dirty Dozen: 12 Scams Most Likely to Arrive Via Bulk Email"*** to publicize the most prevalent UCE scams. The list of scams was culled from a sampling of more than 250,000 spam messages that consumers had forwarded to the FTC's mailbox at uce@ftc.gov. The consumer alert identified the following twelve types of deceptive solicitations and described how each operate: business opportunities schemes; bulk email programs; chain letters; work-at-home schemes; health and diet scams; effortless income; free goods; investment opportunities; cable descrambler kits; guaranteed loans or credit, on easy terms; credit repair; and vacation prize promotions. Nearly 10,000 copies of this consumer alert have been distributed, and it has been accessed more than 35,000 times on the FTC's web site.

D. Considering the Future In Light of Past Experience

In the past year, Commission staff has investigated spamming and the extent to which consumers fall victim to misleading offers. Where staff's investigations revealed significant economic harm to recipients who responded to deceptive UCE, the Commission has taken enforcement action. While neither the Commission's UCE database nor staff's interviews with consumers constitute a representative sample of all UCE and UCE recipients, it is notable that, in the Commission's experience to date, a small percentage of consumers have actually lost money responding to deceptive UCE. However, a deceptive spammer can still make a profit even though very few recipients respond because the cost of sending bulk volume UCE is so low -- far lower than traditional mail delivery. Whether consumers respond to deceptive UCE by either becoming victims or "flaming" senders (*i.e.*, sending angry return emails), forwarding their UCE to the FTC, or automatically deleting all of their UCE, the Commission is concerned that the proliferation of deceptive UCE poses a threat to consumers' confidence in the Internet as a medium for personal electronic commerce.

As government, industry, and consumer interests examine legislative, self-regulatory, and law enforcement options at this important turning point, it is useful to be mindful of lessons learned in the past. Earlier in this decade, the advent of the first and still the most universal interactive technology, 900 number, telephone-based "pay-per-call" technology, held great promise. Unfortunately, unscrupulous marketers quickly became the technology's most notorious users.

Tens of thousands of consumers wound up with charges on their telephone bills for calls to 900 numbers that they thought were free. Others were billed for expensive calls made by their children without parental knowledge or consent.

The FTC and state attorneys general brought dozens of enforcement actions to halt these schemes and warned legitimate 900 number vendors that industry practices needed to improve dramatically. Unfortunately, industry did too little to halt the widespread deception, and Congress enacted the Telephone Disclosure and Dispute Resolution Act of 1992, directing the FTC and FCC to regulate 900 number commerce by issuing rules under the Administrative Procedure Act. The regulations have forced all 900 number vendors into a standard practice of full disclosure of cost and other material terms, and have virtually eliminated the problem of deceptive 900 number advertising. All of this came at a considerable cost, however, because consumers lost confidence in pay-per-call commerce and stayed away from it in droves. Only now, some six years after federal regulations took effect, has there been growth in pay-per-call services as a means of electronic commerce.

The Commission has steadfastly called for self-regulation as the most desirable approach to Internet policy. The Commission generally believes that economic issues related to the development and growth of electronic commerce should be left to industry, consumers, and the marketplace to resolve. For problems involving deception and fraud, however, the Commission is committed to law enforcement as a necessary response. Should the Congress enact legislation granting the Commission new authority to combat deceptive UCE, the Commission will act carefully but swiftly to use it.

Endnotes:

1. The views expressed in this statement represent the views of the Commission. My responses to any questions you may have are my own.

2. 15 U.S.C. § 45(a). The Commission also has responsibilities under approximately 40 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 approximately 30 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. *FTC v. Corzine*, CIV-S-94-1446 (E.D. Cal. filed Sept. 12, 1994).

5. Section 5 of the FTC Act, 15 U.S.C. §45, authorizes the Commission to prohibit unfair or deceptive acts or practices in commerce. The Commission may initiate administrative litigation, which may culminate in the issuance of a cease and desist order. It can also enforce Section 5 and other laws within its mandate by filing actions in United States District Courts under Section 13(b) of the FTC Act, 15 U.S.C. 53(b), seeking injunctions and other

equitable relief. Section 18 of the FTC Act, 15 U.S.C.§ 57a, authorizes the Commission to promulgate trade regulation rules to prohibit deceptive or unfair practices that are prevalent in specific industries.

6. For example, the National Advertising Division of the Council of Better Business Bureaus, Inc., operates the advertising industry's self-regulatory mechanism.

7. For example, the Rule Concerning Cooling-Off Period for Sales Made at Homes or at Certain Other Locations (the "Cooling-Off Rule"), 16 C.F.R. Part 429; the Mail or Telephone Order Merchandise Rule, 16 C.F.R. Part 435; the Trade Regulation Rule Pursuant to the Telephone Disclosure and Dispute Resolution Act of 1992 ("The 900-Number Rule"), 16 C.F.R. Part 308; and the Telemarketing Sales Rule Pursuant to the Telemarketing and Consumer Fraud and Abuse Prevention Act, 16 C.F.R. Part 310.

8. May 1996.

9. The Ad-Hoc Report is available at www.cdt.org/spam .

10. "Header" information, at minimum, includes the names, addresses, or descriptions found in the "TO:", "FROM:", and "SUBJECT:" lines of an email. It also includes the technical description of the route an email traveled over the Internet between the sender and receiver.

11. No. 3:99 CV 181 (W.D.N.C. filed May 11, 1999). This case was originally filed under the caption *FTC v. One or More Unknown Parties Deceiving Consumers into Calling an International Audiotext Service Accessed Though Telephone Number (767) 445-1775*. Through expedited discovery, the FTC learned the identities of the perpetrators of the alleged scam by following the money trail connected to the telephone number. Accordingly, the FTC amended its complaint to specify the defendants' names.

12. A similar scheme that used spam was targeted in *FTC v. Lubell, et al*., No. 3-96-CV-80200 (S.D. Ia. 1996). In that case, the spam urged consumers to call an expensive international number to hear a message that purportedly would inform them about discount airline tickets and how to enter a sweepstakes.

13. No. 399 CV 1272 (CFD) (D. Conn. filed July 7, 1999). Other alleged pyramid schemes that thrived on spam have been targets of FTC enforcement action., *e.g., FTC v. Nia Cano*, No. 97-7947-IH-(AJWx) (C.D. Cal. filed Oct. 29, 1997); Kalvin P. Schmidt, Docket No. C-3834 (final consent Nov. 16, 1998).

14. *FTC v. Consumer Credit Advocates*, No. 96 Civ. 1990 (S.D.N.Y. filed Mar. 19, 1996); *FTC v. Dixie Cooley, d/b/a DWC*, No. CIV-98-0373-PHX-RGS (D. Ariz. filed March 4, 1998).

15. *FTC v. Cliff Cross and d/b/a Build-It-Fast*, Civ. No. M099CA018 (W.D. Tex. filed Feb. 1, 1999); *FTC v. Ralph Lewis Mitchell, Jr.*, No. CV 99-984 TJH (BQRx) (C.D. Cal. filed Jan. 29, 1999); *FTC v. Frank Muniz*, No. 4:99-CV-34-RD (N.D. Fla. filed Feb. 1, 1999); *U.S. v. A. James Black*, No. 99-113 (M.D. Fla. filed Feb. 2, 1999); *FTC v. James Fite*, d/b/a Internet Publications, No. CV 99-04706JSL (BQRx) (C.D. Cal. filed April 30, 1999); *U.S. v. David Story*, d/b/a Network Publications, 3-99CV0968-L (N.D. Tex. filed April 29, 1999); and *FTC v. West Coast Publications*, LLC., CV 99-04705GHK (RZx) (C.D. Cal. filed April 30, 1999).

16. *FTC v. Internet Business Broadcasting, Inc., et al*., No. WMN-98-495 (D. Md. filed Feb. 19, 1998); *United States v. PVI, Inc.*, No. 98-6935 (S.D. Fla. filed Sept. 1, 1998).

17. *TrendMark International, Inc.*, Docket No. C-3829 (final consent Oct. 6, 1998)