

**UNITED STATES  
ANNUAL REPORT ON CONSUMER POLICY DEVELOPMENTS  
FOR 2000**

The US government approach to protecting consumers online relies on a combination of government enforcement of existing legal protections and private sector initiatives. The main US federal government enforcement agency that protects consumers from fraud and deception online is the Federal Trade Commission. Part I of this report focuses primarily on the FTC's efforts to combat fraud and deception online. Part II focuses on consumer education initiatives. Part III focuses on public policy initiatives, and Part IV focuses on private sector initiatives.

**I. COMBATING FRAUD, DECEPTION AND UNFAIRNESS IN THE NEW HIGH-TECH, GLOBAL MARKETPLACE**

**A. Identifying Fraud & Deception**

To identify the most serious forms of fraud and deception in the marketplace, the FTC is making greater use of technology, expanding complaint databases, and sharing data with increasing numbers of law enforcement partners. In the past year, FTC databases have grown dramatically, and FTC staff has recruited a large number of new law enforcement partners at home and abroad. Some examples:

**1. Consumer Response Center**

The CRC is now responding to 10,000 inquiries and complaints a week. Consumers use the FTC's toll-free number (1-877- FTC-HELP), file complaints online and send letters. Last fiscal year, the CRC added 338,000 complaints to the FTC's database.

**2. Consumer Sentinel**

*Consumer Sentinel*, the fraud database established by the FTC in 1997, is available online to law enforcement agencies across the U.S., Canada and Australia. It receives fraud complaints from the FTC's Consumer Response Center and from a growing number of other organizations in the U.S. and Canada. *Sentinel* now contains over 300,000 complaints, and is the richest source of consumer fraud data available to law enforcement agencies. In the last year, the FTC recruited 295 new law enforcement partners, bringing the total number of *Sentinel* users to 1200 individuals from over 250 different law enforcement agencies. Consumers also can tap into this website for a wealth of statistics about fraud. Visitors to the public page of Consumer Sentinel can view data that shows: the scams that garner the most frequent consumer complaints; the scams that cost consumers most; the location of companies complained about, by state and by province; the number of identity theft complaints, by state; the types of identity theft most frequently reported; and how to spot and avoid fraud and deception online and off. The FTC has developed two new Internet sites:

§ ***Soldier Sentinel***: a site where military service members can enter complaints online and receive consumer education. The Defense Department will track complaint data and address the most prevalent forms of consumer harm affecting its members.

§ **Public Sentinel:** a site that gives the general public access to the rich and aggregated data collected through *Consumer Sentinel*, including fraud statistics and trends.

§ **Consumer Planet Sentinel:** a site that gives certain members of the International Marketing Supervision Network (IMSN) access to complaints filed online by consumers via the *econsumer.gov* Web site.

### 3. Identity Theft

The FTC has deployed a toll-free number, 1-877-ID-THEFT, and established a central clearinghouse for ID theft complaints. Building on its experience with *Consumer Sentinel*, the FTC began making the data available to law enforcement partners through an online database. Calls to the FTC's toll-free number have increased dramatically, from 400 calls a week a year ago, to over 2,200 a week today.

## B. Internet Law Enforcement Program

### 1. Recent Law Enforcement Cases

Drawing on *Consumer Sentinel* data, FTC staff is targeting the most pervasive online fraud, and moving quickly to stop large, fast-growing Internet scams. In the past year, the FTC brought over 50 cases involving fraudulent or deceptive marketing practices related to the Internet, bringing the total number of Internet cases filed since 1994 to approximately 200. Among its recent law enforcement actions:

§ **Operation Top Ten Dot Cons**

The FTC led the first and largest global law enforcement sweep in its history, targeting the top 10 Internet scams (based on Sentinel data). Over 250 law enforcement actions were brought by five U.S. agencies and consumer protection organizations from nine countries and 23 states.

§ **Modem Hijacking**

In four recent cases, the FTC has obtained court orders against defendants who have cheated consumers through the use of modem dialer software, i.e., software that disconnects a computer modem from the local Internet service provider, dials an international telephone number, and reconnects the modem to the Internet from some overseas location. In one case, *FTC v. Verity International*, the FTC, within weeks of seeing a dramatic spike in consumer complaints about long distance charges on their telephone bills, sued the company in federal district court. The court entered a temporary restraining order, froze defendants' assets, and later issued a preliminary injunction. The case is still in litigation.

§ **ID Theft**

While most ID theft cases are criminal, the FTC staff systematically examines complaint data for cases within its jurisdiction. A case in point: *FTC v. Martinez*, in which the FTC sued the operator of websites selling online access to templates that could produce high quality false identity documents, such as drivers licenses and birth certificates. The court ordered injunctive relief, including an asset freeze and an order to repatriate assets in foreign countries.

§ **Day Trading**

The FTC, together with the CFTC and the SEC, surfed websites that promised consumers would earn high returns with little risk using the websites= Aday trading@ investment strategies. In six cases this year, the FTC challenged Internet marketers of online Areal time@ investment training; software programs; seminars and trading manuals; e-mail newsletters and mentoring services. The orders bar unsubstantiated profit and earnings claims, and require a cautionary risk disclosure statement.

**2. Internet Training**

To help expand anti-fraud efforts throughout the U.S. and abroad, FTC staff recently launched a program to provide Internet investigation training to other law enforcement agencies. So far, FTC staff has offered 13 Ahands-on@ training programs to over 800 law enforcement personnel representing 20 countries, 26 states, 22 federal agencies and 14 Canadian agencies.

**3. Law Enforcement Coordination**

§ **eConsumer.gov**

The International Marketing Supervision Network, which includes consumer protection law enforcement agencies like the FTC, has launched econsumer.gov, which has two components: (1) a public website where consumers can file cross-border e-commerce complaints, learn about consumer protection in other countries, and obtain tips about shopping safely online; and (2) a password-protected government website where law enforcement agencies can access econsumer.gov complaints and communicate confidentially with agencies from other countries. Fourteen countries and the OECD have signed on to this project.

§ **Law Enforcement Sweeps**

One of the most effective tools in the battle against fraud has been the law enforcement Asweep.@ Since 1995, the FTC has joined with partners in bringing 1567 law enforcement actions in 60 sweeps against fraudulent operators. This includes 376 actions by the FTC. In fiscal year 2000, the FTC led 10 sweeps resulting in a total of 245 actions, including 75 FTC cases.

§ **Identity Theft Victim Assistance**

Following a workshop in October with over 170 participants B victims, consumer advocates, representatives of the financial services industry and credit bureaus, and law enforcement agencies B FTC staff is leading an effort, with our public and private sector partners, to streamline the process for victims to report ID theft and restore their good names.

**4. Fostering International Cooperation**

The number of consumer protection cases with an international component continues to rise; in Internet cases, roughly ten percent now involve some international aspect. To increase its effectiveness in such cases, the FTC has undertaken a number of initiatives.

§ **Information Sharing**

The FTC entered into bilateral consumer protection cooperation agreements with the U.K and Australia.

§ **Partnering with Canada**

The FTC entered into a Strategic Partnership with Industry Canada's Competition Bureau, the Ontario Ministry of Consumer and Commercial Relations and the Toronto Police Service. The partnership already has shut down 12 Toronto-based boiler rooms, obtained \$100,000 in restitution, and announced a comprehensive cross-border credit card protection sweep.

§ **Enforcement Sweep**

As discussed above, nine countries joined the FTC in *Top Ten Dot Cons*, the largest global law enforcement sweep to date.

## II. EDUCATING CONSUMERS, BUSINESSES AND THE PUBLIC IN ORDER TO MAKE MARKETS WORK MORE EFFECTIVELY

Consumer and business education is the first line of defense against fraud and deception. With each major consumer protection enforcement initiative, the FTC launches a comprehensive and creative education campaign. Among our activities last year:

### A. Special Initiatives

§ **www.consumer.gov**

The FTC continues to manage [www.consumer.gov](http://www.consumer.gov) and to recruit new agency members to participate in the site, which offers one-stop access to federal consumer information. In the past year, the number of members has grown from 135 to 174 agencies.

§ **Children's Online Privacy Protection Act (COPPA)**

The FTC launched a special webpage at [www.ftc.gov/kidzprivacy](http://www.ftc.gov/kidzprivacy) to help children, parents, and site operators understand the provisions of COPPA and how the new law affects them. Resources available on the website include guides for businesses and parents, and Asmart surfing tips for kids.

§ **Identity Theft**

The FTC developed an extensive multi-media consumer education campaign to help consumers combat identity theft. Materials include: a comprehensive booklet, *ID Theft: When Bad Things Happen to Your Good Name*; the ID theft website [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft); and a toll-free number 1-877-ID-THEFT. More than 196,000 copies of the booklet have been distributed since its release in late February 2000, and there have been more than 261,000 hits to the dedicated website.

### B. Publications

In fiscal year 2000, the FTC issued 100 consumer protection publications 87 for consumers and 13 for business. It distributed more than 5.3 million print publications to the public, and received more than 5.6 million accesses of publications on the Bureau of Consumer Protection site of the FTC website.

### III. POLICY INITIATIVES

#### A. Privacy

Over the past year, the US has continued its efforts to address consumer concerns about privacy online, and to implement new privacy legislation. Initiatives include:

§ **Children=s Online Privacy Protection Act (COPPA)**

The nation=s first online privacy law went into effect on April 21, 2000, requiring that certain commercial websites give notice of their information practices and obtain parental consent before collecting, using, or disclosing personal information from children under 13. To encourage compliance, the FTC created a website posting COPPA materials for businesses, parents, children, and teachers ([www.ftc.gov/kidzprivacy](http://www.ftc.gov/kidzprivacy)); hosted clinics in Washington and California to assist websites seeking to come into compliance; and filed its first enforcement action, *FTC v. Toysmart*. The FTC also approved the Children=s Advertising Review Unit of the Better Business Bureau (CARU), TRUSTe, and the Entertainment Software Ratings Board as the first COPPA A safe harbor@ programs that enable the private sector to operate under FTC-approved self-regulatory guidelines.

§ **Gramm Leach Bliley Act**

In May 2000, the FTC issued a rule implementing the privacy protections of the Gramm Leach Bliley (GLB) Act. The rule requires that financial institutions provide notice and an opportunity for consumers to A opt-out@ of the sharing of personal financial information with third parties. The rule was issued in coordination with the several other agencies and becomes fully effective in July 2001. Earlier this year, the FTC also announced an initiative to enforce GLB=s prohibition against A pretexting,@ the practice of using false pretenses to obtain customer financial information. The project included a surf of more than 1000 websites and a review of over 500 publications, followed by warning notices to 200 firms whose advertising indicated possible GLB violations. The FTC has also brought three law enforcement actions involving pretexting.

§ **Public Workshops**

In December 2000, the FTC hosted a workshop entitled *The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*. The workshop examined the privacy, security and consumer protection issues raised by emerging wireless Internet and data technologies. In March 2001, the FTC hosted *The Information Marketplace: Merger and Exchange of Consumer Information*. Its purpose was to educate the FTC on issues raised by the creation of detailed consumer profiles through the merger or exchange of data, whether offline or online.

§ **Law Enforcement**

In July 2000, the FTC filed a federal court action against *Toysmart.com*, a failed Internet retailer of children=s toys, to prevent the sale of personal customer information in violation of the company=s privacy policy, which stated that personal information would never be shared with third parties. Earlier this year, as part of a global settlement among various interested parties, Toysmart agreed to destroy the customer information.

- **Safe Harbor**

In June 2000, the United States and the European Commission successfully concluded negotiations on the safe harbor privacy accord. In July 2000, the European Commission determined that the safe harbor principles provide 'adequate' protection as defined by the EU Data Protection Directive. The accord assures the continued flow of personally identifiable information to the participating private sector organizations. On November 1, 2000, the safe harbor framework became effective and Commerce launched a new website ([www.export.gov/safeharbor](http://www.export.gov/safeharbor)) that educates U.S. organizations about the safe harbor, explains how to join, and enables interested organizations to sign up online.

**B. Other Initiatives**

§ **Hague Conference on Private International Law**

The US State Department leads the U.S. Delegation to the Hague Conference of Private International Law, which is negotiating a convention on recognition and enforcement of judgments. The FTC and Department of Commerce provide expertise on consumer and other matters in the Hague Convention negotiations.

§ **Public Workshops**

In June 2000, the FTC and Department of Commerce co-hosted a public workshop on alternative dispute resolution for cross-border online transactions. Most recently, the FTC held a roundtable on this topic. The FTC and the Department of Commerce also issued a report summarizing its June 2000 workshop on alternative dispute resolution for online consumer transactions. Most recently, the FTC held a roundtable on this topic.

- **Free Trade Area of the Americas**

The Department of Commerce, FTC and other U.S. Government agencies participate in the Free Trade Area of the Americas (FTAA) Joint Committee of Experts on Electronic Commerce which has highlighted the importance of consumer confidence online. The group has identified key elements for building consumer confidence in electronic commerce, such as protection from fraud, and from misleading and unfair conduct, and effective means of dispute resolution. The Joint Committee also recognizes the importance of international cooperation in this area and has recommended that consumer protection be a priority agenda item for the next round of discussions.

- **Asia-Pacific Economic Cooperation**

The Department of Commerce and the FTC are actively working with other economies in the Asia-Pacific Economic Cooperation (APEC) forum to promote consumer protection for the online environment through information-sharing activities. The Department of Commerce and the FTC helped organize an APEC workshop on consumer protection in July 2000.

- **US-EU Joint Statement**

The U.S. and the European Union signed a joint statement in December 2000 on the importance of building consumer confidence online and the role of alternative dispute resolution in this process.

## V. PRIVATE SECTOR INITIATIVES

The Better Business Bureau's online division, *BBBOnLine*, has worked with industry, consumer representatives and governments to develop a code of conduct that includes provisions on important issues, such as the disclosure of sale terms, privacy, dispute resolution mechanisms, and non-deceptive advertising. *BBBOnLine* issued its code in July 2000. It has also developed a reliability seal program based on the code which allows web shoppers to check information about companies that carry the seal, and provides assurance that these companies adhere to fair consumer protection standards.

Other private sector organizations, such as the Electronic Commerce and Consumer Protection Group, whose members include industry leaders such as AOL Time Warner, Dell, Network Solutions, AT&T, Visa, Microsoft and IBM, have also begun important efforts to address consumer protection in electronic commerce.

In addition, Hewlett Packard chairs the Consumer Confidence Working Group of the Global Business Dialogue on Electronic Commerce, which has done important work on trustmarks, ADR, and privacy. The Direct Marketing Association provides online briefing sessions to its members on complying with ethical best practices and current regulations that affect the direct marketing industry.

The American Bar Association has formed a Task Force on E-Commerce and Alternative Dispute Resolution that is studying various types of online dispute resolution (ODR) methods and ways in which ODR may effectively be used to settle B2C and B2B disputes.

In April 2001, *BBBOnLine*, the Federation of European Direct Marketing (FEDMA), and Eurochambres, the Association of European Chambers of Commerce and Industry, announced their intention to develop a new international seal or 'trustmark' program based on specific business standards, including dispute resolution."

Finally, to address concerns about unauthorized access to merchant databases, Visa has developed new security requirements for cardholder data. These requirements apply to any entity holding card data -- including web merchants, gateways and Internet service providers. These requirements prescribe how these companies should store, encrypt and grant access to cardholder data. For example, they require Internet merchants to install firewalls, to keep security systems up-to-date, to encrypt stored data, and to use anti-virus software, among other things. These requirements became effective May 1, 2001.