Federal Trade Commission

Remarks of Deborah Platt Majoras[1]
Chairman, Federal Trade Commission
ABA Consumer Protection Conference
Washington, D.C.
January 30, 2007

"The FTC's Consumer Protection Agenda: Strategies for the Present and Future"

I. Introduction

Thank you, Joe, and good morning. It is a pleasure to be here today, and I am delighted that the ABA Antitrust Section is holding its first conference dedicated solely to consumer protection issues. This makes eminent sense, because competition and consumer protection enforcement and policy are complementary sets of tools designed to accomplish the same goals – promoting efficiency, preventing consumer harm, and enhancing consumer welfare. In a competitive marketplace, vendors have strong incentives to supply their customers and potential customers with reliable information. But when those incentives are not enough, enforcement of the consumer protection laws promotes the exchange of complete, accurate, and non-deceptive information in the marketplace in a way that protects consumers' personal data.

[1] The views expressed herein are my own and do not necessarily represent the views of the Federal Trade Commission or of any other Commissioner.

The ABA's growing support for exploring consumer protection issues is commendable, and I am particularly proud that the Antitrust Section sponsors and funds the Janet Steiger Fellowship Project, which provides law students with the opportunity to work in consumer protection departments of state attorney generals' offices throughout the United States. By helping to train the next generation of consumer protection lawyers, the ABA honors the memory of an extraordinary public servant, the late Chairman Steiger.

The range of prominent consumer protection issues that the FTC must tackle is enormous: spam to spyware to false advertising to subprime lending to debt collection to data security to media violence to childhood obesity to the National Do Not Call Registry – to name some of them. And, of course, there are a host of rules that we enforce as well – including, for example, rules that dictate how and where the country of origin must be displayed on socks that are sold in the United States. In setting and executing our agenda, there are several strategies we follow.

A. Consumer protection strategies

First, as a relatively small agency with a large mandate, we have to form partnerships and leverage resources. Our primary partners are the consumers themselves, who field the first line of defense against fraud, deception, and theft. Education empowers that defense, and by working with partners – both public and private – to educate consumers about how to recognize phishing scams or the importance of carefully disposing of sensitive information, we can prevent fraud and save consumers countless dollars. I have made consumer education a top priority at the FTC and, indeed, last October, I chose Carolyn Shanoff – the Director of the FTC's Division of Consumer and Business Education – as the recipient of the annual Chairman's Award, the

highest award available to FTC employees. The materials produced by Carolyn's shop continue to break new grounds in creativity and resourcefulness.

We also partner with other government agencies, like the Department of Justice's Civil Division at the federal level, and the state attorneys general, as well as with our international counterparts. We partner with NGOs, including consumer and interest groups that help identify consumer issues and educate consumers. And we partner with the business community. Effective consumer protection is not a simple matter of pitting consumers against industry. Most businesses recognize consumers as the life blood they are and are eager to create a marketplace in which consumers have confidence. Thus, many businesses and organizations partner, for example, in our consumer education, and assist us in our attacks on spam and other Internet scourges. The FTC, in turn, supports several self-regulatory efforts, which provide enormous market benefits.[2] The universe of self-regulatory organizations includes industry-wide or economy-wide private groups that provide, *inter alia*, certification, product information, complaint resolution, quality assurance, industrial standards, product compatibility standards, professional conduct standards, and complaint resolution. Implemented properly, each can provide efficiencies and other benefits to consumers that otherwise likely would not be possible without some form of government intervention. And although I do not want to minimize the importance of government regulation and enforcement, they do have limitations that must be weighed against their benefits.

Our second strategy is to remain focused on consumer harm and to build our agenda

---

[2] Self-regulation is a broad concept that includes any attempt by an industry to moderate its conduct with the intent of improving marketplace behavior for the ultimate benefit of consumers.

based on areas in which the risk of consumer harm is greatest. Our approach combines aggressive enforcement under existing consumer protection laws, ongoing evaluation of the adequacy of existing policies, and constant new learning. Our efforts in each of these areas create a framework for action directed at preventing consumer harm.

Similarly, our third strategy is to get the facts. One trap to avoid in consumer protection is assuming that one's own views as a consumer can serve as a proxy for other consumer views. We strive to develop policies and execute our work in a way that is balanced, thoughtful, and informed. By carefully researching and understanding the relevant issues, we formulate policies that are based upon evidence rather than conjecture.

Finally, we have to plan for the future and not just respond to the often overwhelming problems of today. By educating ourselves about technological developments, market changes, and globalization, we are better-prepared to respond to the needs of tomorrow's consumers and focus our attention where it is most needed.

Having described some of the principles that are important to the agency, I would like to turn to the issues that are prominent on the agenda and some of what you can expect in the coming year. The issues cover five primary areas: international, data security, technology, health, and support for criminal enforcement.

II. International

A. Realignment

Like competition, consumer protection issues have gone global. Most Commission investigations, transactions, or research projects, now require a close consideration of the potential international components. And rapid increases in technology and globalization have

pushed consumer protection agencies around the world to work together to confront new challenges, such as spam, spyware, and data security.[3] The Internet and modern communications devices such as VoIP, for example, have provided immeasurable benefits to consumers, but have also enabled fraudsters to operate without borders.

Thus, through our comprehensive international program, we must work cooperatively with consumer protection authorities around the globe to likewise work beyond borders. Over the past decade, the FTC has brought many successful cases, often in partnership with our foreign colleagues, against fraudulent telemarketers based in other countries, who target U.S. consumers with advance-fee loan schemes, phony foreign lotteries, bogus business directory listings, and other scams.[4] For example, the Dutch telecommunications authority, OPTA, provided the FTC with information and substantial assistance in *FTC v. Westby*, a spam case involving defendants in the Netherlands. The spammers sent U.S. consumers sexually explicit spam with deceptive subject lines that disguised the content. Following the FTC's action, OPTA brought its own case against the principal Netherlands defendants, raiding the defendants' offices and shutting down their servers. Just last summer, OPTA obtained a final injunction in its case.

Given the heightened importance of international considerations in everything that we do,

---

[3] In connection with our work with the Organisation for Economic Co-operation and Development – OECD – the FTC works with more than thirty different international consumer protection agencies.

[4] *See, e.g.*, FTC Press Release, *FTC Halts Bogus Business Opportunity Scam* (Nov. 16, 2005), *available at* http://www.ftc.gov/opa/2005/11/usabeverage.htm.; FTC Press Release, *Cross Border Con Artist Ordered to Pay $2.9 Million* (June 22, 2005), *available at* http://www.ftc.gov/opa/2005/06/pinacle.htm.

today I am announcing that I have realigned the international functions within the agency. The international consumer protection and competition divisions and the technical assistance program, previously three separate units, are now combined to form the new Office of International Affairs. By combining these functions, we will better take advantage of the strong synergies between the two consumer protection and competition missions, maximize our use of resources, and better coordinate our international work. In the past, for example, the international antitrust group conducted bilateral relations with some of the same countries where the technical assistance group was running programs and the consumer protection group may have been seeking assets in a fraud case. Now our staffs are better able to communicate and share their expertise to make us more effective in all of these functions. Or, for example, OECD has one competition committee and two consumer protection committees. By combining our shops, we can better coordinate our messages and emphasize the strong competition and consumer protection synergies. The new Office of International Affairs will support the Bureaus' investigations and litigation, cooperate with our international counterparts, promote international convergence towards best practices, and coordinate technical assistance efforts.

Further, by creating one international office and elevating the director of this office to the senior staff, we are sending an important message to our international counterparts, as well as to all of our domestic partners, that the Commission, as one agency, recognizes the importance of international cooperation.

Randy Tritell, who has served with distinction in various positions in the Bureau of Consumer Protection, former Commissioner Calvani's Office, and the Bureau of Competition, is the new Acting Director of the Office of International Affairs. Since 1998, Randy has led the

International Antitrust Division and, in that capacity, he has played a major role in ensuring the Commission's high standing in the international antitrust community. He will have three deputies working with him: Hugh Stevenson, Liz Kraus, and Jim Hamill.

B. The US SAFE WEB Act

As many of you know, the Commission recently obtained new and expanded powers that will allow us to cooperate more fully with foreign law enforcement authorities in the area of cross-border fraud and other practices harmful to consumers. The US SAFE WEB Act was passed in the very last minutes of the 109th Congress, was signed into law by the President on December 22, and provides the FTC with updated tools for the 21st century.[5]

The Act gives the FTC enhanced authority in four key areas. First, SAFE WEB authorizes the FTC to share compelled or confidential information – including documents and testimony – with its foreign law enforcement counterparts. Before SAFE WEB, the FTC could only share such information with other U.S. enforcers, not with foreign enforcers. Now, the FTC can exercise its discretion to disclose this information, particularly when such sharing would help the FTC's own law enforcement efforts and help U.S. consumers. This provision will streamline parallel investigations, help avoid duplication of efforts, and possibly speed up

---

[5] *See "FTC Gets Broader Authority to Pursue Foreign Spammers,"* Los Angeles Times (Dec. 26, 2006) *available at* http://www.latimes.com/technology/la-fi-foreignspam26dec26,1,275015.story?coll=la-mininav-technology&ctrack=1&cset=true; *See* FTC Press Release, *Statement of Federal Trade Commission Chairman Deborah Platt Majoras On US SAFE WEB Act Being Signed Into Law By President George W. Bush* (Dec. 26,2006), *available at* http://www.ftc.gov/opa/2006/12/safeweblaw.htm.

investigations.[6] Second, SAFE WEB permits the FTC to use its investigative power on behalf of foreign law enforcement agencies. In some cases, effective enforcement cooperation demands that the FTC reach beyond information already in its files and gather new information on behalf of foreign law enforcement authorities. Before SAFE WEB, the FTC could not have provided such assistance to a foreign agency – even if the foreign agency's investigation would ultimately benefit U.S. consumers. Now, if the FTC determines that the requested cooperation is consistent with its policy goals and resources, it can issue a civil investigative demand to an entity located in the United States and share the information with the foreign agency. The FTC also may initiate a proceeding under an existing federal statute to obtain testimony or documents for use in a foreign or international proceeding.[7]

Third, SAFE WEB enables the FTC to obtain information it otherwise would not receive

---

[6] Certain conditions must be met before we will pass on compelled and confidential information about a common target. For example, we must first be provided with assurances that the information will be maintained in confidence. Also, we must be provided assurances that the information will be used only for investigating or engaging in enforcement proceedings against possible violations of foreign laws prohibiting fraudulent or deceptive commercial practices, or other practices substantially similar to practices prohibited by any law administered by the FTC (except antitrust laws, which are not covered by the Act). Essentially, this means that the FTC will look to see whether the foreign agency is acting under authority similar to the FTC's authority. If these conditions are met, the FTC can exercise its discretion to disclose compelled or confidential information.

[7] Before we use our investigative powers, however, the FTC must receive assurances that the information will be used only for investigating or engaging in enforcement proceedings against possible violations of foreign laws prohibiting fraudulent or deceptive commercial practices, or other practices substantially similar to practices prohibited by any law administered by the FTC (except antitrust laws, which are not covered by the Act). In addition, the FTC must consider whether: 1) the foreign agency would provide reciprocal assistance to the Commission; 2) the use of our investigative powers would prejudice the public interest; and 3) the foreign agency's investigation concerns practices that have caused injury to a significant number of persons.

from foreign entities. On the government-to-government level, it protects the confidentiality of information provided to the FTC by a foreign government agency if the foreign authority requests confidential treatment as a condition of providing the information. This addresses the concern expressed by some foreign government agencies that materials they share with the FTC might be publicly disclosed in response to an inquiry under the Freedom of Information Act, which allows any interested person to request the FTC's records on any matter. Now, under SAFE WEB, the FTC will be able to guarantee confidentiality and thereby obtain some extremely valuable information.[8]

Finally, SAFE WEB contains several provisions that will strengthen the FTC's enforcement relationships both bilaterally and within multilateral organizations. For example, SAFE WEB permits the FTC to spend funds, within specified limits of course, on projects and consultations with cooperative foreign law enforcement organizations. It also permits the FTC to enter into international cooperation agreements when such agreements are required as a condition of reciprocal assistance. Significantly, SAFE WEB also allows the FTC to participate in meaningful staff exchanges with foreign counterparts (both antitrust and consumer protection) – exchanges that have been in great demand, but that we have not been authorized to implement.

We feel a great sense of accomplishment and appreciation now that this law has passed, and the Commission will take advantage of our new tools consistent with our policy goals and

---

[8] This exemption from public disclosure also applies to consumer complaints that the FTC receives from foreign government and private sector sources, as well as consumer complaint information submitted to joint consumer complaint projects such as the international website *econsumer.gov*. This type of consumer complaint information can be extremely useful in investigating cross-border matters, and we believe that our ability to protect this information from disclosure will increase the volume of the information that we receive.

resources. We are looking forward to working with our partners – both domestic and international – in the coming months and years as we begin to use our new authority under SAFE WEB.

III. Data Security and Identity Theft

For more than a decade, protecting the privacy of American consumers has been a top priority at the Federal Trade Commission, and it remains a crucial consumer protection issue. The explosive growth of the Internet and the development of sophisticated computer systems and databases has made it easier than ever for companies to gather and use information about their customers. In addressing privacy concerns, it is important to keep in mind that these new information systems can have tremendous benefits for consumers, who can access customer service hotlines 24-hours-a-day, have easier access to credit, and enjoy many marketplace conveniences that they have come to expect. At the same time, if we do not protect sensitive information adequately, consumers can be harmed and lose confidence in the marketplace. The balance must be carefully struck: ask consumers if they care about privacy, and you will get a resounding "yes;" ask consumers if they will tolerate being inconvenienced, and you will get a resounding "no." This is our shared challenge.

In 1998, the Identity Theft Assumption and Deterrence Act ("the Identity Theft Act") assigned the FTC a unique role in combating identity theft and coordinating government efforts.[9] While we cannot prosecute the crime because we have only civil jurisdiction, we take consumer complaints and implement the Identity Theft Data Clearinghouse, a centralized database of

[9] Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

victim complaints used by 1,300 law enforcement agencies; assist victims and consumers who wish not to be victims, by providing information and education; and educate businesses on sound security practices.

Deterrence of identity theft begins with data security – keeping sensitive information out of the hands of wrongdoers. Data security is important for every kind of organization – whether a company, government agency, or university; whether a mom-and-pop shop or a multinational corporation; whether a high-tech company or a low-tech business. It also is critical to every individual, each of whom must learn to better safeguard their personal data. Of course, not all data breaches lead to identity theft and, in fact, many lead to no harm whatsoever. And not all identity theft results from breaches. But, there is no question that some breaches have led to fraud.

Over the past two years, the FTC has brought 14 enforcement actions against businesses that have failed to provide reasonable data security. None of these cases has been a close call. They include cases against companies that threw files containing consumer home loan applications into an unsecured dumpster; stored sensitive information in multiple files when there was no longer a business need to keep the information; failed to implement simple, low-cost, and readily available defenses to well known Web-based hacker attacks; stored sensitive consumer information in unencrypted files that could be easily accessed using commonly known user IDs and passwords; and failed to use readily available security measures to prevent unauthorized wireless connections to their networks.

Probably the best-known FTC data security enforcement action was our case against

ChoicePoint.[10] ChoicePoint, a data broker, inadvertently sold information on more than 160,000 customers to data thieves who used that information to open up new accounts and commit identity theft. The FTC alleged that ChoicePoint failed to use reasonable procedures to screen prospective subscribers. For example, the company allegedly approved as customers individuals who lied about their credentials, used commercial mail drops as business addresses, and faxed multiple applications from nearby public commercial locations. The Commission obtained $10 million in civil penalties for the FCRA violations – the highest civil penalty ever levied in an FTC case – $5 million in consumer redress for identity theft victims, and significant injunctive provisions that require ChoicePoint to implement a variety of new data security measures.

The ChoicePoint case serves as a lesson in what can go wrong when you fail to conduct due diligence on the entities to which you disclose sensitive consumer information. But I also mention this case to illustrate how companies can respond in a positive and constructive way to "clean up their house" after they suffer a breach. ChoicePoint has instituted structural changes, such as creating the new position of chief privacy officer and centralizing its credentialing processes into a single department.[11] And ChoicePoint announced last year that it no longer would provide full Social Security numbers, birth dates, or other sensitive information to private investigators or other small customers. This decision reportedly cost the company an estimated $15 million to $20 million in lost business, but ChoicePoint executives believed that the risk to

---

[10] *See* FTC Press Release, *ChoicePoint Settles Data Security Breach Charges; To Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress* (Jan. 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.htm.

[11] *See* Gary Rivlin, "Keeping Your Enemies Close," *New York Times* (Nov. 12, 2006) available at http://www.nytimes.com/2006/11/12/business/yourmoney/12choice.html.

the company's reputation of pursuing this line of business outweighed the benefit. I am pleased that ChoicePoint has taken the lessons of its breach to heart and changed its operations to minimize the chances of such a breach in the future.

Last year, President Bush concluded that federal government resources directed at identity theft could be more effectively marshaled through a more comprehensive and coordinated effort. Accordingly, on May 10, 2006, the President established his Identity Theft Task Force, which Attorney General Gonzales chairs and I co-chair.[12] In his Executive Order, the President directed the Task Force to submit to him a strategic plan for fighting ID theft. The 18 federal agencies that comprise the Task Force have been hard at work developing the plan.

Last month, the Task Force issued a request for public comments to supplement the research and analysis already conducted, provide further information about the proposals it is considering, and identify areas where additional recommendations may be warranted.[13] The Task Force sought comments in four areas. First, how to improve data security practices in order to keep sensitive consumer data out of the hands of identity thieves. For example, how can governments move towards reducing unnecessary use of, or reliance on, Social Security numbers? Should the Task Force analyze how Social Security numbers are being used in the private sector? Should there be a national data security requirement on commercial entities that maintain sensitive consumer information? Should there be a national breach notification requirement?

---

[12] *See* FTC Press Release, *FTC Launches Nationwide ID Theft Education Campaign* (May 10, 2006), *available at* http://www.ftc.gov/opa/2006/05/ddd.htm.

[13] *See* FTC Press Release, *Identity Theft Task Force Seeks Public Comment* (Dec. 26, 2006), *available at* http://www.ftc.gov/opa/2006/12/fyi0688.htm.

Second, how can we make it more difficult for identity thieves to use the data they obtain to steal identities? Within this category, the Task Force already has recommended that the government hold workshops on improving authentication of individuals' identities. The FTC will host the first of these workshops this spring, and we will publish a Federal Register notice on this authentication workshop in the very near future.

Third, are there ways that we can better assist victims in restoring their identities and recovering from identity theft? Finally, by improving the ability of law enforcers to prevent, investigate, prosecute, and punish the crime, can we deter identity theft? The comment period closed on January 19, and the Task Force is in the process of reviewing the comments and preparing its strategic plan.

Educating consumers is essential in the fight against identity theft. The FTC recently launched a nationwide identity theft education program, "Avoid ID Theft: Deter, Detect, Defend."[14] The message for consumers is that they can:

- DETER identity thieves by safeguarding their personal information;
- DETECT suspicious activity by routinely monitoring their financial accounts, billing statements, and credit reports; and
- They should DEFEND against ID theft as soon as they suspect it. Quick action is essential.

The Deter, Detect, Defend campaign has been very popular – we have distributed more

[14] *See* FTC Press Release, *FTC Launches Nationwide Id Theft Education Campaign* (May 10, 2006), *available at* http://www.ftc.gov/opa/2006/05/ddd.htm.

than 1.5 million brochures and 30,000 kits.[15] And we have formed many partnerships to help us broaden our reach. For example, the National Association of Realtors, which has 1.2 million members, partnered with the FTC to educate homebuyers. And the U.S. Postal Inspection Service just started a large-scale outreach campaign that is placing the FTC's educational materials on subway cars in Washington DC, New York, Chicago, and San Francisco and that is also placing paid advertising in college newspapers and on campuses around the country.

IV. Technology

Today's global, high-tech companies produce products and services that are vastly different than those produced by more traditional "brick-and-mortar" firms. We continue to direct substantial enforcement resources to problems that plague millions of America's computer users, with the goal not only of finding and prosecuting malefactors, but more broadly of retaining consumers' trust in the Internet. The fight against computer-related fraud requires creativity and substantial resources.

Obsolescence, convergence, interoperability, and digital rights management will continue to result in a wide assortment of new technologies. One consumer protection challenge that arises from such changes is that consumers may not be aware of what the new technologies can do and how they can be used lawfully. Through consumer education, industry and the FTC can help to inform consumers about these new technologies. However, in some circumstances, FTC law enforcement action arising from a lack of adequate disclosure of the limitations on the use of

[15] One component of the campaign is a consumer education kit, which is aimed at helping organizations educate their employees, their customers, and their communities about how to minimize their risk. The kit includes a victim recovery guide, a training booklet, a guide to talking about identity theft, presentation slides, an easy-to-read brochure, and a 10-minute video.

new technologies may be warranted.

A. Sony BMG

A new FTC case addressing music CDs with digital rights management technologies – DRM – illustrates this point. DRM technologies generally limit the ability of consumers to use content, such as software, music, and movies. While there are, of course, legitimate uses of DRM technology, such as protecting intellectual property rights and encouraging innovation, DRM also can raise consumer protection concerns. Consumers may be deceived if the content seller makes a false or misleading material claim about how the content may be used, or if the seller fails to disclose adequately material limitations on DRM-restricted content.

Today, I am announcing an FTC action against *Sony BMG Music Entertainment*. Sony BMG sold CDs that consumers could listen to on any traditional home stereo, portable, or car CD player. Unbeknownst to consumers, however, these CDs contained DRM technology that allowed the music to be played on their computers, but did not permit the music files to be directly transferred to or played on certain portable digital devices, such as an Apple iPod for example. The DRM also limited consumers to making three copies of the music files directly from the original CDs.

In our complaint, we alleged that Sony BMG did not adequately disclose that the DRM software would limit the devices on which consumers could play the CDs or the number of copies they could make. Because ordinary experience with CDs would not lead consumers to expect these limits, and because these limits likely would affect purchasing decisions, the FTC alleged that Sony BMG's failure to disclose adequately these limits was deceptive in violation of Section 5 of the FTC Act. To resolve these allegations, Sony BMG entered into a consent

agreement with the Commission under which it must clearly and prominently disclose to consumers any restrictions on the devices on which its music CDs can be played and the number of copies that can be made. *Sony BMG* stands for the important proposition that if new technologies contain material limitations on their use, including that they are not interoperable so that the product does not perform as expected, then it may be deceptive to fail to adequately disclose the restrictions to consumers.[16]

B. Zango/180 Solutions

The Commission has brought nine spyware enforcement actions in the past two years. These actions have reaffirmed three key principles: First, a consumer's computer belongs to him or her, not the software distributor. Second, buried disclosures do not work, just as they have never worked in more traditional areas of commerce. And third, if a distributor puts a program on a consumer's computer that the consumer does not want, the consumer must be able to uninstall or disable it.

---

[16] In addition to challenging as deceptive Sony BMG's failure to disclose adequately the limits on use resulting from the DRM software, the Commission's complaint also challenged as deceptive Sony BMG's undisclosed inclusion on its music CDs of a proprietary media player, which sent information back to Sony over the Internet about the artists/albums that consumers listen to on their computers and returned targeted advertising. The complaint challenged as unfair the company's practices of causing its DRM software, which exposed consumers' computers to security risks, to be installed on computers without adequate notification and consent, and its accompanying failure to provide a reasonable means to locate and/or remove the software. To remedy these charges, the consent agreement requires, among other things, that Sony BMG, before it collects any information through its media player, disclose that the CD will collect information and/or send back advertising to the computer, and obtain consumers' consent to do so; obtain consumers' authorization before it installs content protection software; provide free of charge a reasonable and effective means to uninstall the software; and reimburse consumers up to $150 to repair damage that resulted directly from consumers' attempts to remove the software installed without their consent. *See* FTC Press Release, *Sony BMG Settles FTC Charges* (Jan. 30, 2007), *available at* http://www.ftc.gov/opa/2007/01/sony.htm.

The Commission illustrated these principles in our most recent spyware settlement with Zango, Inc., formerly known as 180solutions.[17] Zango provides advertising software programs, or adware, that monitor consumers' Internet use in order to display targeted pop-up ads. The consent order settles allegations that the company installed its advertising software programs on consumers' computers without adequate notice or consent. Zango's distributors frequently offered consumers free programs or software, such as screensavers, peer-to-peer file sharing software, and games, without disclosing that downloading it would also result in the installation of Zango's adware. In other instances, Zango's third-party distributors exploited security vulnerabilities in Web browsers to install the adware via "drive-by" downloads. As a result, millions of consumers received pop-up ads without knowing why and had their Internet use monitored without their knowledge.

Moreover, the company deliberately made these adware programs difficult for consumers to identify, locate, and remove from their computers, so consumers were stuck with them no matter how they tried to get rid of them. The company used its adware to send billions of pop-up ads over several years. As part of the settlement, Zango agreed to disgorge $3 million in ill-gotten gains derived from its past actions. The company also agreed to injunctive provisions that will protect consumers against these practices in the future.

In another recent case, the Commission persuaded the U.S. District Court for Nevada to shut down the Media Motor spyware program operated by ERG Ventures, LLC, and its

---

[17] *See* FTC Press Release, *Zango, Inc. Settles FTC Charges* (Nov. 3, 2006), *available at* http://www.ftc.gov/opa/2006/11/zango.htm.

affiliates.[18] The Commission complaint charged that the defendants tricked consumers into downloading malevolent software by hiding the Media Motor program within seemingly innocuous free software, including screensavers and video files. Once installed, the Media Motor program downloaded "malware" that changed consumers' home pages, added difficult-to-remove toolbars, tracked Internet activity, generated disruptive and sometimes pornographic pop-up ads, added advertising icons, altered browser settings, degraded computer performance, and attacked consumers' anti-spyware and anti-virus software.

C. Tech-Ade

As we move through this digital decade, the FTC is committed to understanding the implications of technology changes on privacy and consumer protection – as they are happening or even before they happen. Last November, we gave ourselves a glimpse into the future by convening public hearings on the subject of "Protecting Consumers in the Next Tech-Ade."[19] We heard from more than 100 of the best and brightest in the tech world about new technologies on the horizon and their potential effect on consumers. Just a few weeks ago, I attended the Consumer Electronics Show for the first time, viewing more than 1.8 million square feet of creativity and innovation on display, countless cool gadgets and devices, and a lot of extraordinarily large flat-screen TVs. Then last week, while attending the World Economic Forum, I attended a program in which experts discussed what we can expect from the next

---

[18] *See* FTC Press Release, *Court Shuts Down Media Motor Spyware Operation* (Nov. 13, 2006), *available at* http://www.ftc.gov/opa/2006/11/mediamotor.htm.

[19] *See* FTC Press Release, *Hearings Will Explore Emerging Technologies and Consumer Issues in the Next Decade* (July 26, 2006), *available at* http://www.ftc.gov/opa/2006/07/techade.htm.

generation Internet, dubbed Web 2.0. Avatars and Second Life? Wait a minute, I am still working on my first life!

In a very short period of time, cell phones have evolved from mere telephones into cameras, music listening devices, PDAs, Web browsers, navigation systems, televisions, and even payment devices. Plainly, mobile devices warrant our strong focus. At the Tech-Ade hearings, two cutting-edge technologies involving mobile phones intrigued me. The first innovation is Quick Response – QR – Codes, which is a small pictorial representation that appears in print ads or on billboards. Consumers can choose to have their mobile phone read the QR Codes, which results in the receipt of information on the so-called "third screen" from the advertiser. So, for example, Northwest Airlines could include a QR Code on a billboard advertising Hawaiian vacations, and consumers who choose to read it with their mobile phones would receive information about flights to Hawaii and other travel updates. QR Codes are used in Japan already, and they may be debuting here in the United States soon.

The other innovation is using mobile phones to pay for goods and services. Mobile phones can be equipped with a radio frequency identification device that allows consumers to pay for items simply by passing their phone over a reader. This innovative payment technology has been tested at professional football games and was more popular with fans than the back-up quarterback on a losing team.

Such new technologies hold great promises for consumers and businesses, but also come with new challenges, including privacy and security issues. New contactless payment devices offer great conveniences, but also create opportunities for fraud and a need for consumers to understand how these payment systems differ from existing systems.

Our report on the Tech-Ade conference will be published this spring. The Commission has glimpsed some of what the future holds, and clearly it will bring both new benefits and new challenges. We intend to be ready for it.

V. Health

Of course not all fraud is technology related. Health fraud – often in the form of plain old snake oil – can still be found in the offline world as well as the online world. I am reminded of old Western movies that often featured a traveling "doctor" with dubious credentials, selling some medicine with outrageous marketing hype. The "doctor" would inevitably escape town in the middle the night, and by the time his customers realized that they had been swindled, it was too late. At the FTC, one of our priorities continues to be prosecuting purveyors of modern-day snake oil, making sure that the salesmen do not escape in the middle of the night, and getting money back to consumers. Indeed, in *FTC v. Great American Products*,[20] a lengthy dispute over the terms of the final order ended recently, and was followed by a rapid distribution of consumer refunds. After prevailing in November 2006 in the defendants' appeal on their motion for order modification, on December 19, the contractor mailed refund checks totaling more than $15 million to 130,000 consumers (the average check was for just over $118). In response, we have received gratifying hand-written thank you notes with comments including, "The money came at a great time!" and "there is a God, and through him, there's an agency, people who really care."

Too often, consumers fall prey to fraudulent health marketing because they are desperate

---

[20] *See* FTC Press Release, *FTC Targets Bogus Anti-Aging Claims for Pills and Sprays Promising Human Growth Hormone Benefits* (June 9, 2005), *available at* http://www.ftc.gov/opa/2005/06/greatamerican.htm

for help. Fifty million Americans suffer from a chronic pain condition[21] and have found no effective cure or treatment. Seventy million Americans are trying to lose weight. The FTC will continue to prosecute companies that take advantage of these consumers, whether they are fly-by-night or Fortune 500, and whether they are willing to negotiate or insist on litigating to the bitter end. Let me give you examples of two recent cases. The first is an outright fraud perpetrated on hundreds of thousands of consumers suffering from pain. Andrew Park and his companies advertised the Q-Ray bracelet as a device for relief for all kinds of pain. Through infomercials aired on established cable networks including the Discovery Channel, USA Network, and the Learning Channel, the Q-Ray defendants raked in net sales of $87 million, selling their bracelets at prices as high as $250, a mark-up of more than 650 percent.

Their marketing pitch was sophisticated and brazen. They used all the tricks of the trade – dramatic and moving testimonials, impressive scientific terminology, and medical experts touting glowing reports of scientific tests that proved the efficacy of their product beyond a doubt. In one infomercial, a woman suffering from ovarian cancer spoke of the insufferable pain she endured from multiple rounds of chemotherapy: "There's just some mornings I just can't even get out of bed," she states before tearily describing how the Q-ray bracelet has transformed her life, "I'm just amazed and in disbelief. I'm just excited that, you know, my life is normal again."[22]

Although many consumers were swayed by the sales pitch, a federal district judge was

---

[21] Source: American Chronic Pain Association, "Pain Fact Sheet," *available* at http://www.theacpa.org/pu_main_02.asp.

[22] *FTC v. QT, Inc.*, 448 F. Supp.2d 908, 924-25 (N.D. Ill. 2006).

not. The court rejected defendants purported scientific substantiation, stating that, "Not only did Defendants not have a gold-standard study in their possession, they did not even have a copper-standard study."[23] In fact, one randomized, controlled clinical trial conducted by the Mayo clinic suggested that the Q-Ray bracelet was no more effective in reducing pain than a placebo bracelet.[24]

The court found the defendant companies and Mr. Park guilty of misleading and false advertising, both about the pain relief benefits of the bracelet and about the 30-day satisfaction guarantee promise of a full refund, and ordered them to pay up to $87 million in refunds to consumers – the entire net sales generated by the deceptive infomercials, a big victory for consumers and a strong deterrent for fraudulent marketers.[25] Q-Ray demonstrates that the Commission will not back down from a fight. We invested significant resources and time to litigate this case to the bitter end, and the outcome for the agency and for consumers was well worth it.

The second case I will describe is one of four recent cases in the weigh- loss area. Just a few weeks ago, the FTC announced settlements with the makers of four significant and high-profile weight-control and weight-loss products, Trimspa, Cortislim, Xenadrine, and One-A-Day WeightSmart. In a case against Bayer, we announced a $3.2 million civil penalty settlement of an order violation case for alleged deceptive marketing of its One-A-Day WeightSmart.[26] The

---

[23] *Id*. at 965.

[24] *Id*. at 963.

[25] *Id*. at 975.

[26] *See* FTC Press Release, *Federal Trade Commission Reaches "New Year's" Resolutions with Four Major Weight-Control Pill Marketers* (Jan. 4, 2007), *available at*

product, a multivitamin supplement with a sprinkling of green tea extract added to it, was advertised to enhance metabolism and help consumers control their weight. The $3.2 million civil penalty is the largest civil penalty ever obtained by the FTC in a health claims case.

The Bayer case illustrates that our enforcement efforts against health claims and products are not limited to outright fraud by fringe marketers. The FTC takes action against large, national companies when they step across the line and make exaggerated or unfounded claims for otherwise legitimate products. Further, the case should remind companies that not only does our substantiation standard for health claims require that marketers possess competent and reliable scientific studies, but it also is necessary that those studies match the product being marketed and the claims being asserted. Too often, marketers overlook the second part of that equation, for instance, claiming weight-loss benefits where only metabolism effects have been studied, or marketing a product containing only a fraction of the active ingredient studied.

C. Childhood obesity

Another important issue on the Commission's health agenda is childhood obesity. The statistics on obesity are sobering, and its impact on public health is substantial. For example, more children are developing serious conditions like diabetes. And obesity has even reached the youngest of our children.

In the summer of 2005, the Commission and the Department of Health and Human Services held a joint workshop on the issue of childhood obesity.[27] Our goal was to encourage

---

http://www.ftc.gov/opa/2007/01/weightloss.htm.

[27] *See* FTC Press Release, *Workshop Explores Marketing, Self-Regulation, and Childhood Obesity* (July 15, 2005), *available at* http://www.ftc.gov/opa/2005/07/obesityworkshopma.htm.

industry to respond to the public concerns surrounding food advertising and marketing by taking strong action to modify their products, their marketing techniques, and their messages. Our April 2006 report on the workshop did not attempt to assign blame to food marketers (or anyone else) for the rising obesity rates, and it did not call for advertising bans. Rather, it pointed out that all segments of society – parents, schools, government, health care professionals, food companies, and the media – need to work to help improve our children's health. Given that our focus is on advertising, the report urged industry to consider a wide range of options as to how self-regulation could assist in combating childhood obesity.[28]

A number of companies apparently took our recommendations. On October 16, for example, the Walt Disney Company announced new food guidelines aimed at giving parents and children healthier eating options.[29] And just a few months ago, the Children's Advertising Review Unit, CARU, which is administered by the Council of Better Business Bureaus, announced a new self-regulatory advertising initiative designed to use advertising to help promote healthy dietary choices and healthy lifestyles among American children.[30] Ten leading

---

[28] *Perspectives On Marketing, Self-Regulation, & Childhood Obesity: A Report On A Joint Workshop of the Federal Trade Commission And The Department of Health and Human Services* (April 2006), *available at* http://www.ftc.gov/os/2006/05/PerspectivesOnMarketingSelf-Regulation&ChildhoodObesityFTCandHHSReportonJointWorkshop.pdf.

[29] *See* Bruce Horovitz and Laura Petrecca, "Disney to Make Food Healthier for Kids," USA Today (Oct. 17, 2006), available at http://www.usatoday.com/money/media/2006-10-16-disney_x.htm.

[30] *See* Annys Shin, "Ads Aimed at Children Get Tighter Scrutiny; Firms to Promote More Healthful Diet Choices," *The Washington Post* (Nov. 15, 2006), available at http://pqasb.pqarchiver.com/washingtonpost/access/1162355031.html?dids=1162355031:1162355031&FMT=ABS&FMTS=ABS:FT&date=Nov+15%2C+2006&author=Annys+Shin+-+Washington+Post+Staff+Writer&pub=The+Washington+Post&edition=&startpage=D.1&desc=Ads+Aimed+at+Children+Get+Tighter+Scrutiny.

food manufacturers – including McDonalds, The Hershey Company, Kraft Foods, and Cadbury Schweppes – committed to devoting at least 50 percent of their advertising resources directed to children under 12 to advertising products that represent healthy dietary choices or that prominently include healthy lifestyle messages that encourage physical activity or good nutrition. They also committed to reducing their use of third-party licensed characters and to incorporating healthy lifestyle messages into their interactive games.

Over the past few months, I have observed the reactions of interested parties to these voluntary and self-regulatory efforts. Some argue that the efforts are wholly insufficient and fail to even begin to address the serious issues involved. Others argue that industry has no obligation to change its practices and should not be making any changes in its marketing practices towards kids.

I disagree with both positions. These industry initiatives are commendable, and my hope is that they will prompt competition among food marketers and entertainment companies to use their resources to develop healthy and appealing alternatives and to use their creativity to promote effectively those healthier foods and drinks to children and youth.[31] The other choice, though, for industry to simply say, "not our problem," and to fail to take and execute such initiatives would be a poor choice indeed. We all must work together to improve our children's

---

[31] The Commission's appropriation legislation for Fiscal Year 2006 directed the agency to submit a report on food industry marketing expenditures and activities targeted toward children and adolescents. This report must include an analysis of commercial advertising on television and radio and in print media; in-store marketing, including payments for preferential shelf placement; event sponsorship; promotions on packaging; Internet activities; and product placements in TV programs, movies, and video games. This is a very large undertaking, and the work has begun. Our goal is to get the information the Commission needs to provide the thorough analysis that Congress expects of us, through a process that is no more burdensome than necessary.

health.

VI. Criminal Enforcement

One of the first things that hit me after I started at the FTC was that the frauds we prosecute civilly often are, of course, crimes that should be handled accordingly. Over the past two years, the FTC's Criminal Liaison Unit, or CLU, has stepped up our cooperation with criminal authorities – a dramatic illustration of our efforts to bring the collective powers of different government agencies to bear upon serious misconduct in many consumer protection areas. As a result of these cooperative efforts, for example, more than 40 business opportunity con artists targeted during our 2005 business opportunity sweep – Project Biz Op Flop – have been convicted. And in December, the Commission announced Project Fal$e Hope$, another interagency campaign to stamp out business opportunity fraud, in which the FTC, together with the Department of Justice, the United States Postal Inspection Service, and law enforcement agencies in 11 states, announced more than 100 business opportunity law enforcement actions.

During 2006, CLU reported some outstanding developments. Grand juries charged 71 FTC defendants and their close associates with crimes including mail and wire fraud, bank fraud, conspiracy, money laundering, and tax fraud. Among those charged were Steven Warshak and his company Berkeley Premium Nutraceuticals, the makers of Enzyte, an allegedly all-natural "male enhancement" product. Warshak and Berkeley, defendants in an FTC enforcement action for deceptive health-care claims and unauthorized billing, found themselves charged with more than 100 felony counts in a conspiracy prosecution that began after a referral from the FTC.

During the same period, federal prosecutors obtained convictions of 57 FTC defendants and their close associates. And consumer protection-related crimes continued to draw stiff

sentences. Thirty-three FTC defendants and their close associates received prison sentences totaling more than 259 years, ranging from one year to more than 17 years in prison. CLU's Special Assistant United States Attorney (SAUSA) Program contributed to several of these prosecutions. FTC attorneys, deputized as SAUSAs, handled prosecutions of postal job scammer Spencer Golden (87 months), business opportunity fraudster Clark Sampson (77 months), and bogus advance-fee loan huckster Pedro Gonzalez (66 months).

VII. Conclusion

I have covered a lot of ground today, and have touched on some of the major issues that the Commission's consumer protection program is addressing, that are important to me, and that you can expect to encounter in the coming year. One area that we did not cover, but that is particularly important to consumers and the agency, is financial fraud and abuse. The FTC will continue to bring cases focusing on unlawful debt-collection practices and fraudulent or deceptive credit-related practices – including deceptive lending practices for subprime credit cards and fraudulent debt negotiation schemes – and you should expect to see more activity in this area shortly. And we will continue to address issues ranging from general fraud to spam to media violence to Do Not Call enforcement.

We look forward to working with all of you in the protection of consumers.

I would be happy to take any questions.