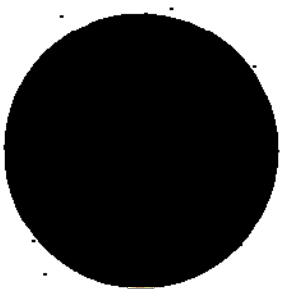

Federal Trade Commission

Protecting Consumers in a High-Tech World
Internet Foundation Lunch
Brussels, April 6, 2005
Remarks by Chairman Majoras

I. Introduction

Thank you. I am delighted to be with you in Brussels today and to introduce you to some of the important work of the U.S. Federal Trade Commission. The FTC is the only federal agency in the United States empowered to promote competition and consumer welfare by enforcing both antitrust and consumer protection laws. The scope of FTC authority is broad, but I would like to focus my remarks this afternoon specifically on some of the FTC's activities to protect consumers in the global electronic marketplace.

To protect consumers, we use a multi-pronged strategy that incorporates aggressive law enforcement, consumer and business education, and research and advocacy. The principal consumer protection statute enforced by the FTC is the FTC Act, which prohibits "unfair or deceptive practices." The statute empowers the FTC to file civil actions in U.S. federal district court seeking injunctive relief against businesses engaged in fraudulent, deceptive, or misleading practices. The FTC also can seek monetary redress for consumers injured by such practices.

Of particular relevance to today's discussion, the prohibition on "unfair or deceptive practices" is not limited to any specific medium. In the past, we have used this language to take action against door-to-door salespeople selling their bogus wares to unsuspecting consumers.

international initiatives in each of these areas.

II. Spam

Spam is one of the most intractable consumer protection problems that the FTC – like you and computer users – has ever faced. The extremely low cost of sending email makes it an appealing marketing channel even for legitimate companies. Unfortunately, low cost combines

to “update” or “validate” account information. The message directs consumers to a Web site that

involved in the OECD Spam Task Force, and we follow very closely the activities of the European Cooperation Network of Spam Authorities (CNSA), led by DG Information Society. We have signed Memoranda of Understanding on spam enforcement cooperation with agencies in the U.K., Australia, and Spain. The FTC is also active in the recent London Action Plan initiative, an informal network of spam enforcers and industry representatives from 20 countries that allows participants to discuss cases, investigation techniques, and educational initiatives. Already, agencies and organizations from 13 European countries participate in the London Action Plan, and participation remains open to spam enforcement agencies and relevant private sector representatives from around the world. Commitments to cooperate, however, will not be enough; we must productively implement cooperative steps to stop spammers.

III. Spyware

Just when we were getting a good start on addressing spam, spyware popped up. The term spyware may be amorphous, but there is no doubt that its negative impact is real. It is hard to find any computer user who has not struggled for hours to remove spyware from his computer.

We recently issued a staff report on a public workshop on spyware we held last year. The workshop explored what spyware is, how it is distributed, and how much harm it causes. We used the information from the workshop to start developing cases, and equally important, to start the discussion of what technology is or may be available to protect consumers. Here, we believe a critical role for government is to encourage technological solutions to help reduce spyware problems.

We have also brought enforcement actions against illegal spyware. We filed our first spyware case in October 2004. In that case, we alleged that the defendants violated the FTC Act

by loading spyware onto consumers' computers that changed their web browsers and barraged them with pop-up advertisements, in addition to installing other software programs without the consumers' knowledge or consent. Then, after creating computer crashes and other malfunctions, the defendants launched pop-up ads that offered to sell an anti-spyware solution for $30. Fortunately, the court granted us a preliminary injunction, which stopped the business from distributing spyware. And, last month, we filed our second case, this one against purveyors of alleged worthless spyware protection software.

Like spam, the problem of spyware highlights the truly global dimension of consumer protection. Purveyors of spam and spyware can operate from anywhere in the world and easily, cheaply, and anonymously target anyone in the world. One tool we need now to combat spam

IV. Information Security

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, employees, and business associates. Recent news reports about the release of consumers' sensitive information from one of the United States' largest commercial information services and a major U.S. bank demonstrate that, if this data is not adequately secured, it can fall into the wrong hands and cause serious harm to consumers. The consequences of security breaches are often severe, ranging from identity theft and unauthorized charges to consumers' accounts, to an increase in spam and "phishing" schemes.

Our primary goal is to encourage all companies to put in place solid information security practices *before* a breach can occur. But where significant breaches do occur, we will continue to determine whether they were caused by the failure to take reasonable steps to safeguard consumers' information. If so, we will take appropriate action. Given the importance of information security to consumers, the FTC has made it one its top law enforcement priorities, and we will be dedicating even more resources to this critical issue.

To date, we have filed five cases challenging false security claims under the FTC Act. In each case, we alleged that the defendants promised that they would take reasonable steps to protect consumers' sensitive information, but failed to do so. For example, last month, the FTC alleged that Petco Animal Supplies promised to keep its customers' information secure, but failed to take reasonable measures to prevent commonly known attacks to its Web site by hackers. The flaws in Petco's Web site allowed a hacker to access consumer records, including

credit card numbers. As with the Commission's prior information security cases, the settlement requires that Petco implement a comprehensive information security program for its Web site.

The FTC also has a central role in educating consumers and businesses about the risks of identity theft and assisting victims and law enforcement officials. The FTC maintains a Web site and a toll-free hotline staffed with trained counselors to advise victims on how to reclaim their

you today.