Federal Trade Commission

Opening Remarks of Deborah Platt Majoras
Chairman, Federal Trade Commission

"Maintaining Momentum in the Fight Against Identity Theft"
National Cyber Security Awareness Summit
Washington, D.C.
October 1, 2007

I. Introduction

Good morning. I am pleased to have this opportunity to help kick off National Cyber Security Awareness Month. Summits like this provide fertile ground for new ideas to germinate and grow. I hope that today we can plant the seeds for developing new approaches to increase cybersecurity awareness. I am delighted to be here with Greg Garcia, the Department of Homeland Security's Assistant Secretary for Cybersecurity and Communications. Although our missions differ in certain important respects, our efforts are complementary, and we share the common goal of ensuring that we in public service do everything in our power to address cybersecurity threats.

Consumers continue to be concerned about cybersecurity and identity theft. One recent survey revealed that more than 90 percent of adults fear that their identities might be stolen and used for unauthorized transactions.[1] Over a third of those surveyed were not confident that companies are taking appropriate steps to protect their personal information. Unfortunately, a recent survey of information technology professionals suggests that consumers are right to be

[1] *See* News Release, *Most Americans Worry About Identity Theft* (April 3, 2007), *available at* http://interactive.zogby.com/index.cfm.

concerned. Over 40 percent of those surveyed believed that their organizations were not doing an adequate job of protecting confidential information.[2] In 2007, these numbers are unacceptable.

Recent news reports reinforce these concerns. A recent survey of on-line banking customers revealed that nearly 1 in 5 respondents had been victims of identity theft or fraud.[3] Another recent survey estimated that consumers lost more than $7 billion over the last two years to viruses, spyware and phishing.[4] And news reports in the past few weeks indicate that millions of customers of two major online businesses may have had their personal information compromised. The reports describe a host of exotic-sounding cyber attacks that may have been at play - Trojan horses, phishing, spear phishing, money mules, spyware, and, ultimately, account theft. Plain old, non-exotic-sounding theft, a crime in any era. While we know that organizations increasingly are reinforcing their data security, given all of the reports of breaches, it nonetheless is hardly surprising that consumers fear that the information they provide will be improperly disclosed or, even worse, lead to identity theft and account fraud.

Today's summit is intended to devise and examine new ways to address cybersecurity awareness and prevention. The FTC supports this effort and continues to confront these issues on several fronts.

II. Identity Theft Task Force

As you likely know, last year the President established his Identity Theft Task Force,

---

[2] *See* Press Release, *New Research by Oracle and Ponemon Institute Shows Organizations Can Improve Processes to Protect Against Privacy Breaches* (June 18, 2007), *available at* http://www.oracle.com/corporate/press/2007_jun/oracle-ponemon-survey.html.

[3] *See* News Release, *Study Shows Banks Could Increase Profitability by $8.3 Billion Per Year if Stronger Security Measures Implemented, available at* http://www.tricipher.com/news/pr134.htm.

[4] *See* News Release, *U.S. Consumers Lose More Than $7 Billion to Online Threats, Consumer Reports Survey Finds, available at* http://www.consumersunion.org/pub/core_telecom_and_utilities/004797.html.

charging 17 federal departments and agencies with the mission of developing a comprehensive national strategy to combat identity theft.[5] As co-chairman of the Task Force, I have had the opportunity to work with representatives from across the U.S. government, including the Department of Homeland Security.

In April, the Task Force submitted its Strategic Plan with 31 recommendations, organized around the life cycle of identity theft, to the President.[6] The first series of recommendations is targeted at identity theft **prevention** by keeping sensitive data out of the hands of criminals and making it more difficult for them to use such data when they do manage to steal it. For example, the Plan recommends several actions in both the public and private sectors to limit the unnecessary use, transfer, and display of Social Security numbers. It also encourages the development of national data security and breach notification standards. In addition, the Task Force recommends a national awareness campaign to teach consumers how to protect their information.

The second set of recommendations relates to **victim recovery** - helping victims to reestablish their financial identities. Some of these recommendations include the implementation of a standard police report for victims, and assistance and training for "first responders" and victim assistance counselors.

Third, the Plan recommends a number of actions to strengthen law enforcement's ability to **deter and punish** identity thieves, including stronger penalties and enhanced cooperation among local, state, federal, and foreign authorities.

---

[5] Exec. Order No. 13,402, 71 FR 27945 (May 10, 2006).

[6] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* ("Strategic Plan"), *available at* http://www.idtheft.gov.

The Task Force has made considerable progress in carrying out the recommendations. In the area of data security, the government is investing significant resources to bring its own house in order. The Office of Management and Budget (OMB) has developed a list of the "Top Ten" things about data security that government agencies should be aware of and required all agencies to develop a formal incident response plan by September 30 (yesterday), aided by guidance that the Task Force provided.

Endeavoring to set an example, the FTC has developed an improved information privacy and security program, spearheaded by our Privacy Steering Committee (PSC), a network of senior staff and managers from throughout the Agency who are led by our Chief Privacy Officer and Chief Information Security Officer. I can tell you that they worry about cybersecurity - a lot. The PSC establishes and communicates FTC policies from data collection to data disposal, covering every place information can be found, from major systems and applications, to faxes and file folders. Our Breach Notification Response Plan was completed this past June. This Plan provides a high-level strategy to handle data security breaches, including those incidents posing a potential risk of identity theft. FTC employees are required to report any confirmed or potential breaches of nonpublic information, an obligation reinforced at a week-long awareness campaign the agency held in July. The Plan also establishes the FTC Breach Notification Response Team, whose mission is to provide advance planning and guidance, and a recommended course of action in response to a breach. To date, two dozen federal agencies have requested materials from the FTC's privacy program and plan to implement practices from it.

In other Task Force work, the Office of Personnel Management is developing unique federal employee identification numbers in an effort to move away from unnecessary uses of

social security numbers. Similarly, the Defense Department, which has used social security numbers since the 1960s, is migrating away from their use and overhauling its identification system. The FTC is leading efforts to develop a comprehensive record on the use of Social Security numbers in the private sector, with the goal of developing recommendations on how we can limit the availability of this valuable information to criminals while at the same time preserving the many beneficial purposes for which SSNs are collected, used, and shared. The Commission solicited and received more than 300 public comments on this issue and will hold a workshop on SSN usage on December 10 and 11.[7] Many of the comments we received reflect the dilemma we face: while the public is rightly concerned about misuse of their Social Security numbers, these unique identifiers have many important uses - - uses that enable hospitals, banks, and universities to link us accurately to our data. At the workshop, we will explore ways to make the SSN less valuable to identity thieves, while still retaining its use in detecting fraud and ensuring accurate matches of data. This past Spring, the Commission also hosted a workshop on authentication, bringing together academics, business groups, consumer advocates, and others to explore new developments in the rapidly changing field of identity management. FTC staff is working on a report that will describe what we learned at this workshop, such as information about technological and policy requirements for developing better authentication processes.

With respect to victim assistance, the Commission has already implemented many of the Task Force recommendations, including publishing a "Victims' Statement of Rights,"[8] and launching a standard police report for identity theft victims. The FTC and DOJ are coordinating

---

[7] *See* http://www.ftc.gov/opa/2007/07/ssn.shtm.

[8] *Available at* www.idtheft.gov.

with the American Bar Association to support more victim assistance through pro bono programs and are developing a training curriculum for victim assistance counselors in the court system. And just last week, the FTC worked with DOJ, the Secret Service, the U.S. Postal Inspection Service, and the American Association of Motor Vehicle Administrators to provide training for local law enforcement in the Chicago area; in December, we will conduct similar training in North and South Carolina.

Finally, with respect to criminal law enforcement, every U.S. Attorney's Office now has designated an identity theft point of contact, and they are coordinating with state and local law enforcement to prosecute cases and conduct outreach. In fact, some offices recently announced cases against people who used malware to engage in identity theft, as well as cases involving the low-tech bribing of employees to obtain data to commit identity theft.

III. Law Enforcement

A. Data Security

The FTC remains vigilant on the law enforcement front, battling inadequate data security practices, spam and spyware. Over the past few years, the FTC has brought 14 enforcement actions against businesses for their failure to provide reasonable data security. A number of these cases have addressed an issue of particular relevance to the cybersecurity community - the failure by companies to implement readily-available defenses to well-known Web-based hacker attacks, such as Structured Query Language (SQL) injection attacks. As these cases make clear, companies may not ignore their responsibilities to take precautions against reasonably foreseeable cyber-crime techniques. In bringing these cases, we hope that, by now, the message is clear: Be aware of common and well-known security threats and protect against them.

Other data security cases have involved less complex but still significant security deficiencies, such as storing sensitive information in multiple files when there was no longer a business need to keep the information; storing such information in unencrypted files that could be easily accessed using commonly-known user IDs and passwords; and failing to use readily available security measures to prevent unauthorized wireless connections to their networks.

Two points bear emphasizing in connection with our data security cases. First, none of the cases was a close call - in each case, vulnerabilities were multiple and systemic, and in most cases simple, low cost measures were readily available to prevent them. Second, the violation in each of the cases was not the data breach itself, but the failure to take reasonable precautions to prevent it. The Commission today has more than two dozen open data security investigations; where appropriate, we will take enforcement action, continuing our efforts to ensure that companies maintain reasonable safeguards to protect sensitive consumer information.

B. Spam and Phishing

The Commission has maintained an aggressive anti-spam program, bringing nearly 100 cases against 243 companies and individuals engaged in deceptive and unfair spamming practices in the last ten years. This summer the Commission hosted a workshop, "Spam Summit: The Next Generation of Threats and Solutions," to examine how spam has evolved and what stakeholders can do to address it.[9] We learned that, in some respects, consumers seem to be getting the message about the importance of protecting themselves. For example, a *Consumer Reports* study previewed at the Summit indicates that fewer consumers are replying to spam, and more of them

[9] http://www.ftc.gov/bcp/workshops/spamsummit/index.shtml.

are using spam blocking technology and firewalls on their home computers.[10] In the bad news category, however, workshop participants described how spam is being used increasingly as a vehicle for more pernicious conduct, such as phishing and the delivery of viruses and spyware. This spam goes beyond mere annoyance to consumers – it can result in significant harm by shutting down consumers' computers, enabling keystroke loggers to steal identities, and undermining the stability of the Internet. As one of our staff stated during the two-day event, the Spam Summit was aptly named. When climbing a mountain, the Summit is a place where you can look back to see where you have come from; you can also look forward to see where you are going. Indeed, the Spam Summit took stock of the excellent work stakeholders have done thus far to combat spam. It also re-affirmed a forward-looking commitment to step up law enforcement efforts, improve technological tools, and enhance public-private cooperation, both domestically and internationally.

We are endeavoring, for example, to target "phishing," to which too many consumers still are falling prey. According to the *Consumer Reports* study, the number of consumers who submitted personal information in phishing-related identity theft scams remained constant since last year, at about 8 percent of the study respondents.[11] In three of our cases, we have targeted "phishers" - identity thieves who used deceptive spam to con consumers out of credit card numbers and other financial data. In these cases, we charged the defendants with violating the

---

[10] As reported by Jeffrey Fox, Technology Editor of *Consumer Reports*, on Day 2 of the Spam Summit. A copy of this portion of the transcript is available at: http://www.ftc.gov/bcp/workshops/spamsummit/draft_transcript_day2.pdf. A copy of the study from *Consumer Reports* is available at http://www.consumerreports.org/cro/electronics-computers/computers/internet-and-other-services/net-threats-9-07.

[11] *See* http://www.consumerreports.org/cro/electronics-computers/computers/internet-and-other-services/net-threats-9-07/overview/0709_net_ov.htm.

FTC Act, which prohibits unfair and deceptive practices, and the Gramm-Leach-Bliley Act, which protects the privacy of consumers' sensitive financial information. Of course, given that the underlying behavior in phishing scams is typically criminal, we have worked with DOJ. For example, in one of our phishing cases, *FTC v. Zachary Hill*, the Department of Justice brought a parallel criminal case leading to a 46-month prison sentence for the defendant.[12]

The Commission is redoubling its efforts to stop illegal spam and phishing schemes. Phishing is one practice that drives me crazy, because if we could just educate every consumer and train them to hit "delete" rather than "reply," we could wipe this out. First, in the upcoming months, we plan to convene a half-day anti-phishing roundtable with the goals of identifying opportunities for outreach and securing commitments from key stakeholders in the anti-phishing community, including consumer and industry groups.

Second, we plan to produce a video with important information about phishing. With your help, it should reach millions of people across the Web.

Third, we are working with the anti-phishing community to mobilize members of the financial sector and revitalize consumer education outreach efforts, including promotion of the OnGuardOnline materials. In our view, working with the financial sector will be critical, given that financial services is the industry sector most targeted by phishers.[13]

Finally, we continue to encourage the industry's adoption of domain-level email authentication as a significant anti-spam and anti-phishing tool. At our Spam Summit this summer, we learned that industry has made great strides with email authentication - 50 percent of

---

[12] *See* http://www.ftc.gov/os/caselist/0323102/0323102zkhill.shtm.

[13] According to the Anti-phishing Working Group, the financial services sector was the most targeted industry sector at 95.2% of all attacks in the month of June.

legitimate email is now authenticated.[14] A recent study indicates that Internet Service Providers are now applying negative scoring to unauthenticated messages.[15] We look forward to working with industry as they continue to advance in their email authentication efforts.

C. Spyware

The Commission also has been active on the spyware front, bringing eleven 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.

The Commission's settlement against four defendants in the Media Motor case, filed just last week, illustrates these principles. These defendants used malware to silently download dozens of unwanted programs onto more than 15 million consumers' computers on others' behalf. These downloaded programs, among other things, hijacked the Internet browser home page; installed a toolbar that displayed disruptive advertising; disseminated a number of pop-up ads, including pornographic ads; monitored Internet use; collected personal information; and even disabled security software. Moreover, once installed, many of these programs were very difficult to remove from computers.

In settling the case, the defendants agreed to clearly and conspicuously disclose the name and function of all software to be installed and provide an option to prevent the installation. They

---

[14] *See* http://www.ftc.gov/bcp/workshops/spamsummit/draft_transcript_day2.pdf. at 85.

[15] *See* http://www.dmnews.com/cms/dm-news/e-mail-marketing/42251.html.

also agreed to refrain from distributing software that "interferes with a consumer's computer use." and making any false or misleading representations in connection with any product or service. The defendants will pay a total of $330,000 in disgorgement. The Commission will continue to bring enforcement actions in this area.

IV. Consumer and Business Education

I mentioned consumer education as a way to wipe out phishing. In fact, ensuring maximum cybersecurity more generally requires a trained populace. The FTC last year launched a nationwide identity theft consumer education program - "Avoid ID Theft: Deter, Detect, Defend."[16] The message for consumers is that they can "deter" identity thieves by safeguarding their personal information; "detect" suspicious activity by monitoring their financial accounts, billing statements, and credit reports; and "defend" against ID theft by taking action as soon as they suspect it. This campaign includes both direct-to-consumer outreach materials, as well as a kit with multi-media training materials for employers, community groups, and others to teach their constituents. The FTC to date has distributed more than 2.6 million brochures, has recorded more than 3.2 million visits to the program's Web site, and has disseminated 55,000 training kits. Several organizations, including the National Association of Realtors, have co-branded and reproduced copies of the materials to distribute among their members. And, you may have seen posters for the campaign on subway cars in Washington, New York, Chicago, and San Francisco.

The FTC also sponsors an innovative multimedia website, OnGuardOnline, designed to educate consumers about basic computer security.[17] The site features interactive quizzes,

---

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

[17] *Available at* http://onguardonline.gov/index.html.

articles, and videos on a range of topics – such as spyware and phishing – as well as information about other resources available to help consumers navigate the world of cybersecurity. OnGuardOnline was developed in partnership with other governmental agencies and the technology sector. The Department of Homeland Security, for example, provided a series of computer security alerts, which can be found on the site.

We branded OnGuardOnline independently of the FTC so that other organizations may make the information their own and disseminate it in ways that reach the most people and suit their particular needs. Since its launch in late 2005, OnGuardOnline has attracted more than 3.5 million visits. Microsoft, Ebay, the National Consumers League, California's Bank of Stockton, and the Web site of my home state, the Commonwealth of Pennsylvania, are just a few of the entities that are either using or linking to OnGuardOnline materials.

In an effort to educate businesses as well, earlier this year the FTC released a new business guide on data security, which has proven to be very popular.[18] The guide articulates the key steps that businesses should take as part of a sound data security plan:

- "Take stock" - Know what personal information you have in your files and on your computers,
- "Scale down" - Keep only what you need for your business,
- "Lock it" - Protect the information that you keep,
- "Pitch it" - Properly dispose of what you no longer need, and
- "Plan ahead" - Create a plan to respond to security incidents.

We also are putting the final touches on an interactive online tutorial based on the data

[18] *Available at* http://www.ftc.gov/infosecurity/.

security business guide. Through the tutorial, users will learn about data security from business people in a fictional small town. They share experiences and find answers to common questions about protecting personal information in their care. For example, in one scene, a sales executive gets practical advice on scaling down the amount of personal financial data about his customers he keeps in his files and on his company's computer network. Business employees who watch the tutorial can create and download their own customized tip sheets so they can apply the same advice in their office. Look for the tutorial at www.ftc.gov/infosecurity in about a month.

Also, as recommended by the Identity Theft Task Force, Commission staff is planning to hold regional data security conferences for businesses. We anticipate launching these conferences early next year.

As you can probably tell, I am proud of the efforts we have undertaken in consumer and business education. Other federal agencies also have made great efforts. For example, DHS's Computer Emergency Readiness Team, or US-CERT, provides a valuable resource to consumers and businesses in identifying cyber threats, preventing cyber attacks, and limiting the damage done by such attacks. But it is not enough. We need every stakeholder joining in the outreach efforts so that we can hit every consumer who touches a computer. It is only through complementary efforts targeted at many different audiences that we will have the most impact.

V. Conclusion

As all of us recognize, data security and identity theft continue to present evolving and complex challenges. Data thieves are constantly developing new ways to overcome security measures and obtain sensitive personal information. Much like the best football coaches, we must

constantly update our playbook with new defensive schemes to counter the opposing team's shifting offensive plans. But an updated playbook is insufficient by itself. The playbook will work only if every member of the team is properly educated and trained to execute the plays. And this is where this summit comes into play. We are here with the common goal of educating members of our team - consumers, businesses, educational institutions, and government agencies - to ensure that all are best prepared for the season ahead, whatever the identity thieves and fraud artists throw at us. I am excited to help open this campaign, and I know that, working together, we can expect a winning season ahead.