Remarks of Lydia B. Parnes
National Cyber Security/Identity Theft Awareness Summit
October 1, 2007

I want to thank the National Cyber Security Alliance for inviting me to speak on this panel. NCSA has been a great partner to the FTC on many of our consumer and business education efforts. Most notably, NCSA has been a great supporter and promoter of our OnGuardOnline consumer education website that Chairman Majoras talked about this morning. If I had to sum up NCSA's contributions in a sentence, I'd say that NCSA has done a great job of keeping the online safety network "networked."

In her remarks, Chairman Majoras provided an excellent overview of how the Commission and the President's Identity Theft Task Force are approaching the critical issue of cybersecurity awareness. There are two basic target audiences for our cybersecurity message: organizations that collect and maintain sensitive data (both public and private), and consumers.

On the consumer education front, Chairman Majoras described the FTC's extensive and highly successful consumer awareness and education campaigns, including our Deter, Detect, Defend and OnGuardOnline campaigns. But, while consumer self-protection is necessary, it isn't sufficient to solve the problem. Consumers can take numerous steps to protect their sensitive personal information, such as limiting disclosure of sensitive information to businesses; securing home computers with anti-virus and anti-spyware software and firewalls; exercising caution in using the internet; and disposing of sensitive information properly. But consumers can do very little to protect their information once they've entrusted it to an organization - at that point, it's up to the organization to make sure the information is well protected.

This morning, I would like to focus briefly on this other audience for our cybersecurity message - the organizations that have consumers' data and should be protecting it. Over the past few years, the Commission has conducted a great deal of outreach to the business community, as have many others both in government and the private sector. We have held workshops covering critical data security issues such as proper authentication, and on the perils of spam, spyware and phishing. We have distributed volumes of guidance and advice, much of which the Chairman highlighted in her keynote address. And, I and my colleagues have spoken to and met with countless business groups, business leaders, and the private bar. We will continue this dialogue and outreach with regional data security workshops targeted to local businesses in the coming year.

Certainly by now, most everyone must have at least a general understanding of the cybersecurity problem and the need to address it. Indeed, all you have to do is pick up the newspaper and read about the latest data security breach. No doubt, an increasing number of businesses and other organizations have "gotten the message" on data security. We have come a long way even in a couple of years when the first major breaches hit the press.

Yet, surveys continue to show that too many organizations are not doing enough to protect sensitive data. The Chairman mentioned one survey in which 40% of IT professionals said their organizations were not doing an adequate job of protecting confidential information. Here is another: a survey in May of 700 C-level executives, managers and IT security officers in mid to large firms that yielded the following results:[1]

---

[1] *See* Press Release, *Scott & Scott, LLP and Ponemon Institute Announce the Results of Survey Assessing the Business Impact of Data Security Breach*, (May 15, 2007), *available at* www.ponemon.org/press/Ponemon_Survey_Results_Scott_and_Scott_FINAL1.pdf.

- 87% of their companies had experienced a data breach.
- Only 43% had an incident response plan in place at the time.
- As a result of the breach, 95% of the companies had to notify consumers about the breach, 74% lost customers, and 32% experienced a decline in share value.

If that isn't enough to motivate you to protect your data, I don't know what is. And yet, even after the breach, many of these companies failed to undertake basic security measures:

- 46% did not encrypt data on portable devices.
- 63% failed to implement a document disposal plan.
- 46% failed to provide security training to employees.

How can this be?

Of course, we can certainly do more outreach - and we intend to - but there is a more fundamental question that remains: What are the barriers to getting organizations to devote the resources and management attention on data security commensurate with the threat?

I like the top ten tips Scott McNealy from Sun Microsystems came up with for Chief Privacy Officers to get CEOs to pay attention to privacy and security challenges.[2] Some of his tips included:

- Tell the boss the auditor lost his personal data on a stolen laptop.
- Publish his recent NetFlix orders.
- Post the boss's college report card, assuming he graduated.
- Remove all sticky notes, with passwords, from his computer screen.

But, more seriously, we all need to think about better ways to motivate organizations to do the right thing. From the Commission's standpoint, education is critical, but law enforcement

---

[2] *See Top Ten Ways to Make Privacy the Boss's Concern, available at* www.sun.com/aboutsun/executives/mcnealy/myvoice.jsp.

may be even more so. A couple of years ago, after we had brought our first cases under the Safeguards rule, the head of a major trade organization told my staff that he had been trying to convince his members ever since the rule went into effect that they needed to do more to protect their data, but no one listened until the FTC starting suing companies. With apologies to Duke Ellington: "It don't mean a thing, if it ain't got that **sting."**

We are often told by corporate IT officers that senior management is unwilling to budget resources without a tangible return on investment. Let me suggest that the return on investment for data security spending is not having your company's name in the headlines of *USA Today* as the latest subject of a security breach or an FTC lawsuit. As the MasterCard commercials would say: "Priceless."

I would like to leave you with four tips that businesses would be well-advised to follow as they consider how to meet their cybersecurity challenges and stay off the pages of *USA Today*.

First, if you make claims about data security, be sure that they are accurate. The FTC has challenged companies' claims that they had strong security procedures in place to protect consumer information when the companies did not have even the most basic security measures in place.[3]

Second, be aware of well-known and common security threats and protect against them. In many of our cases, we alleged that companies failed to protect their customer information from a simple and well-known type of hacker attack.[4] In others, we have challenged failures to

---

[3] *See, e.g., Microsoft Corporation*, Docket No. C-4069 (2002), *available at* www.ftc.gov/os/caselist/0123240/0123240.shtm; *Petco Animal Supplies, Inc.*, Docket No. C-4133 (2004), *available at* www.ftc.gov/os/caselist/0323221/0323221.shtm.

[4] *See e.g., Guidance Software, Inc.*, Docket No. C-4187 (2006), *available at* www.ftc.gov/os/caselist/0623057/index.shtm.

protect data from obvious low-tech security threats such as dumpster diving.[5]

Third, know with whom you are sharing your customers' sensitive information. One of our most significant security cases was against a data broker – Choicepoint – that sold 160,000 consumer files to identity thieves posing as clients.[6] In its complaint, the Commission alleged that the company lacked reasonable procedures to verify the legitimacy of its customers.

Fourth, do not retain sensitive consumer information that you do not need. In two cases we brought involving DSW Shoe Warehouse[7] and BJ's Wholesale Club,[8] the companies stored full magnetic stripe information unnecessarily, long after the time of the transaction when the companies no longer had a business need for the information. The magnetic stripe information was unencrypted and had weak access controls. As a result, thieves were able to hack into a single store's database and from there into the company's central database, where they obtained hundreds of thousands of credit card numbers and security codes.

Following these four steps may not guarantee success against cybersecurity threats but it will certainly put you in the best position to avoid harm to your business and customers. I look forward to hearing more about these issues and to working with NCSA and all of you to meet the cybersecurity challenges we face.

---

[5] *See, e.g., Nations Title Agency, Inc., Nations Holding Company, and Christopher M. Likens*, Docket No. C-4161 (2006), *available at* www.ftc.gov/os/caselist/0523117/0523117.shtm.

[6] *See United States of America (for the Federal Trade Commission) v. ChoicePoint, Inc.*, FTC File No. 052-3069 (2006), *available at* www.ftc.gov/os/caselist/choicepoint/choicepoint.shtm. In settling the matter, ChoicePoint agreed to pay a $10 million penalty and another $5 million to compensate identity theft victims.

[7] *See DSW Inc.*, Docket No. C-4157 (2005), *available at* www.ftc.gov/os/caselist/0523096/0523096.shtm.

[8] *See BJ's Wholesale Club, Inc.*, Docket No. C-4148 (2005), *available at* www.ftc.gov/os/caselist/0423160/0423160.shtm.