Spam, Authentication and Ensuring the Promise of the Internet:
Welcoming Remarks on Day Two
FTC/NIST Email Authentication Summit

November 10, 2004, 8:30 a.m.

Good Morning:

I am Jon Leibowitz – the newest Federal Trade Commissioner. Thank you all for being here at this very early hour to participate in the email authentication summit. I want to open the second day of the summit by encouraging everyone in this room with an interest in email authentication – whether an IP-based model, a signature-based model, or some other technology or combination of technologies – to work together to develop the tools necessary to help solve the spam problem. This a goal we all share and one that is attainable through cooperation and creativity.

With that said, let me say that I am delighted to be here this morning. Let me also thank the National Institute of Standards and Technology for co-hosting this event, for doing the "heavy lifting" yesterday in moderating some of the technical panels, and for helping us sort through the various authentication proposals and acronyms, from BATV, IIM and Domain Keys . . . . to SIDF and CSV (not to be confused with CVS).[1]

As a courtesy to my colleagues on the Commission, let me add the usual disclaimer: The views I express here today are my own and are not necessarily those of the Federal Trade Commission or any other individual Commissioner.

The Federal Trade Commission has a special interest in the electronic marketplace. In

[1] BATV = Bounce Address Tag Validation; IIM = Identified Internet Mail; SIDF = Sender ID Framework; CSV = Client SMTP Validation; and CVS = ubiquitous national drug store chain.

the past decade, a whole new free-flowing exchange of goods and information has emerged, with huge benefits for consumers. As this cyber-market has expanded exponentially, so too have technological challenges and the creativity of those engaging in cyber-fraud, theft, and misrepresentation. Simply put, we can't let spam, spyware, and spoofing undermine the promise of the Internet.

Most people have a visceral reaction to spam – and it's no wonder why. Consider the statistics – experts say that spam accounts for as much as 70 percent of all email and costs businesses $10 billion a year – much of that passed on to consumers. It also costs consumers countless hours in wasted time and immeasurable frustration. Consider also that the vast majority of spam is deceptive – from false headers and phony identities to fraudulent offerings. Just look at the spam in our in-boxes:

- Ads for discount software – sometimes spelled w-e-a-r.   (Here's a tip: if they can't spell it, you probably don't want to buy it from them);
- Unbelievably low-interest rate mortgages. (Look, Mom, I'm already approved!);
- Phishing expeditions by anglers looking to steal your financial account information and maybe even your identity; and
- Ads for "herbal viagra" and so-called "vitality products" that won't extend anything – except the time you spend on the computer trying to get rid of the spam, as well as the pop-up ads, spyware, viruses, worms, and other pestilence that it seems to breed.

Spam is a problem that has literally hit home with me. I have two young girls – ages seven and nine – who have just started to navigate the Internet, have their own email accounts, and are often online, "IM'ing" their friends. I am extremely concerned – and more than a little nervous – that they will encounter this type of brazen, offensive spam – or something far worse.

Obviously we need a multi-faceted approach to combat this serious problem. Aggressive law enforcement is one part of the solution. The Commission has brought dozens of spam-related cases, and the CAN-SPAM Act has given the Commission – and ISPs – some additional tools to go after illegal spammers.

In addition, last month the Commission filed its first ***spyware*** case, against defendants who allegedly downloaded spyware, changed consumers' home pages and search engines, delivered a barrage of pop-up ads, and caused CD-rom trays to open and close. Most outrageous, the defendants then sold anti-spyware products to the very same consumers to fix the problems the defendants originally caused.

We hope that the Commission's law enforcement efforts against spam and spyware will send a strong signal to Internet crooks that we are on the beat. It was also heartening to see AOL, Earthlink, Yahoo and Microsoft join together last month to file more CAN-SPAM lawsuits.

Beyond law enforcement, we need consumer and business education to increase awareness and help users secure their computers – and avoid being spammed and scammed. The Commission is vigorously pursuing education initiatives, and some corporations and consumer organizations are also beginning to build public awareness. These efforts are crucial.

But law enforcement and education alone cannot do the trick. And rather than a "do not email" registry that could cause as many problems as it would solve – at least until the technology improves – we do need new approaches beyond filtering, which can be both over- and under-inclusive.

For example, one of my staffers emailed a draft of my remarks home with “spam summit” in the subject line, and it was caught by her spam filter, filed along with the rest of the daily deluge of spam. The next day she emailed another draft home, labeled just “summit.” Again, caught in the spam filter, but at least retrievable.

As discussed at length during yesterday’s session, several authentication systems have been developed and show promise – including both IP-based and signature-based approaches. I am pleased to see that market forces appear to be working. In determining and deploying some type of authentication system – or combination of systems – we need to ensure ***balance*** and ***flexibility***, to accommodate various types of users.

- To begin, any authentication system should protect the privacy, anonymity and free expression of noncommercial email users. Political dissidents, victims of domestic abuse, and others must be able to communicate freely and anonymously.
- In addition, we don’t want to create unnecessary burdens or expenses for individuals and small business users – any system has to be open, easy to use, and backwards-compatible.
- Finally, we need to remember that spam is a ***global*** problem that requires a global solution. We should be mindful of international implications, standards, and compatibility issues. In this vein, it was encouraging last month to see the Commission join with government agencies from around the world to adopt a global Action Plan on Spam Enforcement.

Accommodating all these goals and interests won’t be easy but the benefits are important – so we need to move ahead, and quickly. This two-day summit is intended to foster a dialog among industry, government, and consumers, to explore various authentication approaches, and hopefully to come to some resolution. Although figuring out a workable authentication system is not a panacea, it will help:

- Authentication will help reduce phishing – spam artists will have a harder time hiding their identities and posing as legitimate businesses;
- It will help ISPs reduce their reliance on their spam filters;
- It will help ISPs and law enforcement determine the domain where the spam comes from, improving our chances of identifying, locating, and catching deceptive spammers — and deterring others; and
- Most important, authentication will help ensure consumer trust and confidence in the Internet – crucial elements to the long-term viability of e-commerce.

* * * *

Last week the Commission received a joint letter from dozens of technology companies – a clear indication that industry stakeholders are beginning to take steps to collaborate on authentication strategies to surmount the seemingly insurmountable spam problem. This summit is an excellent opportunity to share these ideas with additional companies and constituencies.

Let me conclude by turning to all of you – technology wizards, policy gurus, consumer advocates, and Internet leaders. Work up your plans and work out your differences. If we have competing authentication systems that do not work together, we may not have any that work. Let's not allow this to be just another spam discussion that rounds up the usual suspects. Instead, this is a unique chance for the private sector to craft a market-based approach to ensure the continued success of the Internet. To be blunt, you don't want government to write the rules of the road here. You want to write them yourself.

So finish your coffee, go back to the summit, and please continue to work together in the future to benefit consumers.

Thank you.