

November 5, 2004

To be sent to each FTC Commissioner / NIST
Title
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580

Dear Commissioner xyz,

We applaud the FTC's continued leadership on anti-spam enforcement and education and view the upcoming authentication summit as an important step forward in protecting consumers from spam. As you are well aware, spam continues to increase and remains one of the greatest sources of consumer and business complaints. Spammers continue to find new ways to compromise the security, integrity and viability of the Internet and e-mail, thereby undermining users' trust and confidence. As an industry, we are working together to fight this common enemy. We continue to invest heavily in innovative technologies while collaborating on enforcement actions and customer education to ensure the reliability and deliverability of legitimate e-mail.

Despite our progress, spammers have become more creative and deceptive. Fraudulent practices such as spoofing and phishing are increasingly robbing individuals of their security, privacy and financial assets. No one company can solve this problem alone and this is why we are working together to lead the adoption of email authentication technologies, to help protect users and restore their online trust and confidence. Authentication by itself will not stop spam but it enables a wide range of technologies and approaches beyond the content of the message based on the accreditation and reputation of the sender.

We believe that successful deployment of e-mail authentication will be achieved in phases, incorporating multiple approaches and technologies. Today there are two primary methodologies: IP-based solutions such as Sender ID Framework (SIDF) and signature-based approaches such as Yahoo's DomainKeys and Cisco's Identified Internet Mail. Both have a place in deploying authentication for email.

The comparison is fairly simple. IP-based approaches are easier to deploy while signature-based approaches show the promise of broader applicability but are early in their deployment cycle. A recommended strategy is to 1) adopt SIDF today and publish Sender Policy Framework (SPF) text records and 2) as signature solutions mature, adopt them complementing SIDF to achieve a higher level of authentication.

Recognizing the complexity of effecting change in the global e-mail infrastructure, we believe there are numerous benefits of having multiple authentication techniques. By deploying both IP and signature-based solutions, we will ultimately have a more robust solution to address the ranges of platforms, user environments and deployment requirements worldwide.

SIDF is a combination of SPF (Sender Policy Framework) and the Microsoft Caller ID for E-mail draft proposals that have evolved over the past several months, reflecting input from the IETF MARID working group and a number of industry stakeholders. SIDF has been enhanced, providing deployment flexibility, accommodating a combination of platform, application, and licensing choices including backward compatibility to over 100,000 domains that have published SPF records. As we speak, this technology is in early deployment and shows significant promise. and therefore, businesses and ISPs should initiate the implementation of SIDF and publish their records today.

As industry leaders, we share a responsibility for protecting users from the blight of online threats. While many of us compete in the marketplace, we stand united in our fight against spam and phishing and in the support of e-mail authentication standards. We are committed to deploy the Sender ID Framework by publishing our records and advance signing technologies such as Cisco's Identified Internet Mail and Yahoo's Domain Keys which can be rapidly deployed to meet the needs of consumers and enterprises worldwide.

For additional information to review and implement these e-mail authentication alternatives visit www.truste.org/authentication.

Sincerely,

Amazon.com Inc	Anti-Phishing Working Group (APWG)	Association for Competitive Technology (ACT)	Barracuda Networks
CipherTrust Inc.	Cisco Systems Inc	Cloudmark Inc.	Constant Contact
Digital Impact Inc	DoubleClick Inc.	EarthLink Inc.	eBay Inc.
Email Service Provider Coalition (ESPC)	Equifax Inc	Goodmail Systems Inc.	Habeas Inc.
IronPort Systems Inc.	MailFrontier Inc.	Microsoft Corporation	Meng Wong
Port25 Solutions Inc	. Postini Inc.	Return Path, Inc.	Scalix Corporation
Sendmail Inc	SKYLIST Inc.	StrongMail Systems	Symantec Corporation.
Teros Inc.	The Go Daddy Group		The Open Group
TRUSTe	Tumbleweed Communications Corp.		VeriSign Inc.