Comment #: 39

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

September 30, 2004

VIA ELECTRONIC MAIL

Mr. Donald S. Clark
Secretary
Federal Trade Commission
Room 159-H
600 Pennsylvania Avenue, NW
Washington, DC 20580

RE: E-Mail Authentication Summit – Comments (Matter No. P044411)

Dear Secretary Clark:

Microsoft submits these comments regarding the November 9 and 10 E-Mail Authentication Summit (the "Summit") sponsored by the Federal Trade Commission ("FTC" or the "Commission") and the National Institute of Standards and Technology ("NIST"). As a leading technology company – and especially as a provider of Internet access and e-mail services – we are committed to ensuring that our customers feel comfortable using e-mail to communicate, and that e-mail remains a viable medium for business and personal communications. For these reasons, Microsoft supported passage of the CAN-SPAM Act and continues to work with government officials and other industry members to address the spam problem. Microsoft commends the FTC and NIST on their decision to hold the upcoming Summit as a complement to the Commission's thoughtful and comprehensive report to Congress on the proposed Do-Not-E-Mail Registry. We appreciate this opportunity to submit written comments in advance of the Summit.[1]

As the Commission has recognized, a key component of any countermeasures to spam and online fraud is the development of an e-mail authentication system. Although existing filters look at the origin of an e-mail message as part of the process to determine whether that message is spam, there is currently no guarantee that a message originated from whom and where it says it did. The "Sender ID Framework" technology that Microsoft and other industry leaders have developed and are testing is an authentication system that will help not only to address this problem, but also curb other abuses associated with the transmission of forged and unsolicited commercial e-mail.

---

[1] Microsoft also submits today under separate cover a Request To Participate in the Summit.

In the Notice of the upcoming Summit, the FTC and NIST solicited comments on a number of questions regarding authentication systems. While these questions introduce a variety of challenging and complex issues that we address below, our most important comment is that authentication technology is an essential part of a comprehensive solution to end the spam epidemic – a solution that we are committed to pursuing. Just three days ago, for example, Microsoft joined with Amazon.com to file suit against a Canadian spamming ring. We believe these Canadians spoofed the Microsoft Hotmail and Amazon domain names in millions of e-mails as part of a phishing scam to surreptitiously gather personal information about consumers by misleading them to believe that either Microsoft or Amazon was collecting that information. The widespread implementation of authentication systems will complement this aggressive enforcement, targeted legislation, public education, industry best practices, and other technological improvements (particularly advanced filters) in the battle against this type of spam and online fraud. As an international corporation that is a leader in the development of authentication technologies, a major Internet access and e-mail service provider, a software company, and an online business, Microsoft has been affected in numerous ways by the proliferation of spam and its progeny. But more fundamentally, spam is a persistent plague on consumers and continues to be the number one complaint we receive from our e-mail customers.

I. THE SENDER ID FRAMEWORK

Spam was once considered a mere nuisance. Today it continues to threaten to overwhelm Internet e-mail and undermine user trust and confidence, as well as to disrupt the millions of businesses that depend on online commerce and e-mail marketing. To be controlled, spam must first be isolated and filtered. That, in turn, requires identifying the true source of the message. As the FTC and NIST are aware, however, e-mail today is typically sent over the Internet without any authentication of the sender or the computers acting on his or her behalf – a fact that is routinely exploited by spammers in the variety of ways detailed in the Notice.

As a result, filtering junk e-mail can be an error-prone activity. Some spam that appears to originate from legitimate senders slips though filters. Worse, these spoofed e-mails can be used for the types of fraud and phishing scams that the Commission, Microsoft and others are now prosecuting. On the other hand, e-mail from legitimate senders is often blocked because their Internet addresses have been spoofed and their reputations tarnished.

The Commission's Notice of the Summit describes two proposed private market authentication systems. One of these proposals, Sender ID, is based on a combination of Microsoft's "Caller ID for E-Mail" and the Sender Policy Framework ("SPF"). Sender ID involves three steps:

1. E-mail senders (of all sizes) publish one time the Internet protocol ("IP") addresses of their outbound e-mail servers in the Domain Name System ("DNS") according to the Sender ID specification.

2. Recipient e-mail systems examine each message to determine the purported responsible domain.

3. Recipient e-mail systems search the DNS for the list of outbound IP addresses of that domain, and then check whether the IP address from which the message was received is on that list. Once widespread deployment is achieved, if no match is found, the message is not authenticated and has likely been spoofed. During the initial phases of deployment, such authentication failure would likely be included in filtering technologies and algorithms designed to detect spam.

While the Sender ID system is not a silver bullet to counter spam, it does represent a significant industry initiative to detect spoofed domains, reducing both spam and phishing attacks while increasing the reliability and deliverability of legitimate e-mail.

The Sender ID Framework has been designed to meet five core requirements.

- Ease of Adoption. A key goal of this proposal is rapid and broad adoption. We want all Internet domains to quickly publish their outbound e-mail server IP addresses. Therefore, any technical implementation will need to operate within the capabilities of existing software wherever possible. It will not always be possible to implement this proposal without changes to some software, but Sender ID has been designed to keep such changes to a minimum to facilitate adoption. The overarching goals have been ease of implementation, rapid deployment and a minimum of costs to e-mail senders.

- Scalability. Any implementation must also be able to scale up to meet the needs of the largest ISPs and down to the smallest office or home mail server. An authentication system must support organizations that have hundreds or even thousands of e-mail servers as well as those that have just one. Such a system must also support entities that outsource their e-mail servers to another organization.

- Fairness. Authentication systems must also equitably distribute the costs of compliance. Today, the costs of detecting and remedying spoofing are borne entirely by the recipients – the receiving e-mail system and the addressee. Any technical implementation must rectify this imbalance. Organizations that wish to protect their domain names from spoofing should bear part of the cost burden, while organizations that wish to accurately determine whether or not messages they receive have been spoofed should bear a corresponding cost.

- Openness. The technical implementation must be openly published so that any organization wishing to comply with its provisions may do so. This openness is essential to widespread adoption, which in turn is necessary to end the spam epidemic.

- Extensibility. Finally, an authentication system must be able to adapt to changing practices and technology. The technical implementation must therefore allow for the publication of new or additional information about an organization's e-mail policies and practices should this be required in the future.

The Sender ID Framework does not prevent spam from being sent, but it does make spam much easier to detect by providing a more reliable answer to the fundamental question of who sent a given message. This framework helps e-mail senders protect their domain names, their reputations and their brands; enables e-mail recipients to filter junk e-mail more accurately; helps prevents the use of spoofing to perpetrate phishing scams; and provides a basis for additional filtering decisions based on the reputation and e-mail behavior of the sender.

E-mail authentication standards such as Sender ID will have both a direct and an indirect effect on reducing spam. The direct effect of e-mail authentication is that messages which fail e-mail authentication tests may be blocked or negatively weighted by a receiving organization's spam filters. Given past behavior, we expect spammers to adapt to e-mail authentication schemes fairly rapidly – indeed, there is some evidence they are already doing so by sending mail from an address that is either registered in the DNS (and passes authentication tests), or does not participate in an authentication scheme (resulting in neither a pass nor a fail result from an authentication test). As a result, this direct effect of blocking mail that fails an authentication test may be relatively short-lived.

The indirect benefits, however, are long-term and substantial. First, authentication proposals like Sender ID enable senders to take affirmative steps to protect their domain names, and often their brand names, from spoofing. This helps to preserve the reputations and value associated with these names. Second, they provide a foundation for additional scrutiny of the sender. Once a receiving e-mail server can identify the origin of a message with some certainty, it can apply additional experience-based criteria to help determine whether or not to trust the sender and accept messages from that source. For example, receiving servers could examine the historical pattern of message transmission from that sender, noting that a sudden high volume of mail from a previously unknown sender might be suspicious. Receiving servers could also examine the track record of the sender with respect to end-user complaints, message rejection, or rates of spam detected. These indicators could be incorporated into the overall spam filtering process. E-mail authentication thus provides a basis for inferences about the reputation and past behavior of the sender that could not previously be drawn – thereby improving the success rates of filters and decreasing spam and its associated costs.

Technology alone, however, will not solve this problem. A holistic approach that also includes industry collaboration, legislation, enforcement, and education is necessary to shift the burden from the user to the spammer, resulting in an increase in the reliability of e-mail and of the Internet. This approach also requires that any proposed authentication standard be supported on a global basis, because spam transcends and traverses national borders. Collectively, these measures will help to substantially reduce

the amount of junk e-mail delivered to users' mailboxes and optimize users' overall online experience.

II. KEY ISSUES

The FTC and NIST have recognized that the authentication component of this solution raises a wide range of challenging questions. The Notice seeks comment on issues in several areas, including: (1) Technology and Operation; (2) Implementation; and (3) Intellectual Property. Microsoft has anticipated and investigated many of these issues throughout the development of Sender ID, and as explained below, we do not believe that they pose a significant impediment to the widespread adoption of authentication systems.

A. Technology and Operation

The Notice solicits comments on a variety of operational issues involving authentication systems, including their effect on existing Internet protocols, their interoperability, and their implications for specific types of users. As noted above, we have designed the Sender ID program to maximize operational ease, and we believe that an authentication procedure can be incorporated smoothly into the e-mail process for the entire spectrum of users.

- Effect on Internet Protocols. E-mail authentication proposals must supplement rather than replace existing Internet protocols to facilitate widespread adoption. E-mail is the most widely used Internet application, and radical changes to existing protocols are therefore highly unlikely to achieve the widespread deployment required in order for them to succeed. Sender ID is thus designed for easy adoption.

- Effect on Existing Hardware and Software. While Sender ID is being designed to operate under existing conditions to every extent possible, such a system cannot be implemented without some enhancements to e-mail software. In particular, receiving e-mail servers need to be modified to perform the necessary authentication checks, and in some cases to present to the user the results of those checks. Senders may also need to make some changes to both software and administrative procedures. Most e-mail authentication proposals, including Sender ID, require publication by domain owners of certain information concerning their authorized e-mail servers. Sender ID also requires modest changes to the e-mail software used by sending servers in certain situations – mainly to those servers that perform e-mail forwarding. As more and more organizations adopt e-mail authentication techniques, pressure will mount on those who are not participating, because their e-mail will be subjected to greater scrutiny and will be at a greater risk of being blocked by spam filters. Thus, over time, upgrades to existing software will become necessary. While we would encourage upgrades to be made as quickly as possible to realize the benefits that e-mail authentication provides, we recognize that for many organizations software upgrades require significant budgetary,

administrative and technical planning – and we are designing Sender ID with these concerns in mind.

- Effect on All Customer Segments. We believe that any authentication solution needs to be supportable by and compatible with all types of customers and e-mail users. This includes the individual consumer as well as small, medium and enterprise businesses that today rely on e-mail for communication, commerce and productivity.

- Handling of Unauthenticated Messages. Operators of receiving e-mail servers will in all likelihood set their own policies regarding the handling of unauthenticated messages. We believe that over time unauthenticated messages will be subjected to more rigorous scrutiny and filtering procedures. However, we also believe it unlikely that many organizations will block unauthenticated e-mail messages solely because they are unauthenticated; as noted above, authentication is just one part of the technology-based solution to identify and filter spam.

- False Negatives and Positives. Virtually any authentication scheme is susceptible to both false positives and false negatives, and Sender ID is no exception. False positives – where legitimate mail fails an authentication check – are most likely to arise when the identity being validated belongs to an administratively distinct organization from the mail server that transmits the message, as in the case of mail forwarding. False negatives – where spoofed mail passes an authentication check – can occur when a legitimate sender is infected by an e-mail virus (so-called "zombie" machines), or when several apparently responsible identities are deliberately inserted into a message so that one identity is validated while another spoofed identity is presented to the user. This is why we believe that e-mail authentication mechanisms will in general not be used in isolation but rather will provide additional input into spam filtering decisions. Used in combination with other empirical indicia of reliability, e-mail authentication can enable more vigorous and accurate spam filtering.

- Interoperability. Most e-mail authentication proposals are interoperable. In fact, there may be some benefit to using more than one such system to provide additional protection against spam. However, there are limits to the number of authentication schemes that can practically be deployed. Just as most members of the public possess more than one form of identification (e.g., Social Security Number, driver's license, passport) but would probably balk at carrying numerous different ID cards, it is likely that e-mail systems operators will similarly resist deploying too many authentication schemes. We therefore expect that market forces will winnow these schemes down to a small number.

- Effect on E-Mail Forwarding Services. E-mail authentication schemes like Sender ID that tie authentication to the IP address of the sending e-mail server require each message to carry an identity within the sending server's administrative domain. Forwarded messages that lack such an identity are indistinguishable from spoofed mail. Thus, under Sender ID, e-mail forwarders are required to modify a forwarded message so as to provide a locally-controlled identity upon which the receiving side may perform an authentication check. One easy way to do this is to add a "Resent-From" header to the message indicating that identity. This header can then be used in authentication checks performed by the receiving server.

- Effect on Particular Users. Internet mail provides enormous flexibility in the way e-mail is transmitted and routed. Diverse services such as mailing lists, outsourced e-mail, and web-generated e-mail have flourished by leveraging this flexibility. In general, these services can be characterized as "e-mail intermediaries" between the original author of an e-mail message and the ultimate recipients of the message. These intermediary services legitimately send mail on behalf of their users or customers. The intermediary service may act on behalf of the message sender (in the case of mailing lists or web-generated e-mail) or on behalf of the recipient (in the case of forwarding services). E-mail authentication proposals must accommodate these different e-mail service offerings or they will fail to be adopted. That said, the operators of these services must bear their fair share of the cost and responsibility for making e-mail authentication succeed. Sender ID is designed to accommodate the existing behavior of these e-mail intermediaries where possible, and to require only minimal changes to their operation when necessary. Specifically, these intermediaries must place an identity in each message that is under the administrative control of the service's own domain. This allows the authentication to tie an identity in the message back to the domain's authorized outbound e-mail servers.

B. Implementation

Microsoft recognizes that widespread implementation of e-mail authentication raises significant concerns about cost, timing, and potential side effects. We believe that our Sender ID program has been designed to address these issues.

- Cost. The main implementation costs for Sender ID are related to administration and software upgrades. There is a small administrative cost involved in publishing and maintaining information about authorized outbound e-mail servers in the DNS. This nominal cost is borne by domain owners. Operators of a DNS server can expect some increase in the size of their DNS databases and in the load placed on those servers by receiving e-mail systems querying for additional information. Receiving e-mail systems will require some software upgrades to perform the

required authentication checks. And some e-mail senders, particularly mail forwarders, will also require software upgrades in order to ensure that their messages comply with the new authentication requirements. These short-term and often one-time costs, however, are minimal in comparison with the long-term savings and benefits that authentication provides.

- Timing. While we would hope for and encourage rapid deployment of Sender ID, experience shows that changes to large systems occur gradually. Sender ID is designed to permit this, while delivering benefits to those who adopt it quickly. Domain owners can publish information in DNS today to begin to protect their domains from spoofing. As soon as some large ISPs, such as Hotmail, begin performing authentication checks, there will be greater incentive for more domains to publish and for more receivers to perform checks, which will expedite widespread adoption.

- Side Effects. The side effects of authentication should be minimal. Performing Sender ID authentication checks will consume modest amounts of computer processing power and will place some additional load on sending domains' DNS servers. We do not, however, believe that there will be any significant impact upon e-mail transmission times.

C. Intellectual Property

To be effective, any authentication system must be able to be adopted widely and easily. That can only happen if the technical specifications work, and if they are readily available. Microsoft has developed the Sender ID standards with those goals in mind.

- Open Standard. Any authentication system requires cooperation between senders and recipients of e-mail. For that reason, we believe that specifications for these systems must be publicly available and widely implemented – which is why our Sender ID specifications have been published as Internet Drafts at the Internet Engineering Task Force ("IETF"). A technical interoperability specification is an open standard when it has been ratified in an open, consensus-based process. Defining characteristics of open standards include: (1) the ratified specification is made publicly available without contractual restrictions on access; (2) the organization that has ratified the open standard has a transparent Intellectual Property policy; and (3) the ratifying organization will not ratify the specification as an open standard unless patent holders of identified essential patent rights have agreed to license such essential patent rights on reasonable and non-discriminatory terms to anyone who wished to make, use or sell implementations of the open standard. These characteristics are common among standards approved by the American National Standards Institute and internationally-recognized standards bodies. IETF's standards policy has each of these characteristics. Because e-mail is the most widely used Internet application, Sender ID or

any other proposal will need to be broadly adopted to be an effective solution. Consequently, the Sender ID specifications must be freely available to anyone without contractual restrictions on their access. Moreover, any essential intellectual property rights needed to make, use or sell implementations of Sender ID must be available to all implementers and users under licenses with reasonable and non-discriminatory terms. The Sender ID Framework satisfies these conditions because its specifications are published by the IETF, and because the essential intellectual property rights disclosed to the IETF have been made available on reasonable and non-discriminatory terms that are also free of royalties and other fees. (The IETF working group on Sender ID has not reached consensus on the proposal and has suspended its work for now – a decision which is being appealed – but the disclosure of intellectual property rights to IETF and its publication of Sender ID Framework specifications endures and thereby satisfies the conditions for an open standard.) The test of whether Sender ID or any other proposed solution is an open standard is not whether it has been ratified through an open-consensus based process, but rather whether the proposal can be widely adopted – indeed, many successful industry standards are not ratified by a standard-setting organization.

- Proprietary and Patent Rights. Microsoft has disclosed to the IETF that it has filed US and foreign patent applications that include claims that could cover some portions of the Sender ID specification if those claims are granted.[2] Consistent with this declaration – and going even further than offering to license essential patent rights on "reasonable and non-discriminatory terms" – Microsoft has made a Royalty-Free Patent License for Sender ID available online.[3] The terms of this license can be accepted by anyone at anytime, now or in the future, and will extend to all of Microsoft's essential patent rights needed to implement Sender ID – not just the essential patent rights that could issue from these patent applications. Microsoft's publicly-available patent license provides the industry sufficient assurance that anyone can adopt Sender ID without fear of owing Microsoft royalties or other fees for use of essential Microsoft patent claims, although this license does not cover other patent rights that might be owned or controlled by parties other than Microsoft and that may be needed to make, use or sell implementations of Sender ID or other proposals being considered by the IETF. Like Microsoft, other parties subject to the IETF policy should disclose their patent rights and their

---

[2] Microsoft's patent declaration can be found at http://www.ietf.org/ietf/IPR/microsoft-ipr-draft-ietf-marid-core.txt.

[3] This license can be found at http://download.microsoft.com/download/b/d/3/bd3b5463-c461-409e-b29f-512218d3f3e6/SenderID_License-Agreement.pdf.

willingness to license those patent rights for any other proposed authentication standard submitted to the IETF.[4]

- Intellectual Property Obstacles. We are not aware of any proposed standard that would require the use of any particular party's goods or services. However, the Sender ID proposal may be covered by Microsoft patent rights if those rights are granted by the relevant patent offices. As noted above, Microsoft has already made available a patent license at no cost to anyone for any Microsoft patent right that is essential to make, use or sell implementations of Sender ID. Microsoft cannot, however, confirm whether it has patent rights in other technology nor, obviously, whether any other party has patent rights that might be needed to make, use or sell implementations of other proposed authentication standards.

* * *

Microsoft appreciates this opportunity to provide comments to the FTC and NIST about the development, use and implications of authentication technologies. We look forward to discussing these issues further at the upcoming Summit, and to continuing to work with government and industry to end the threat posed by spam.

Sincerely,

Michael Hintze
Senior Attorney
Microsoft Corporation

[4] More information on the disclosure of patent rights for parties subject to the IETF is provided at http://www.ietf.org/ipr.html.