Comment #: 42

TRUSTe *Make Privacy Your Choice*

Filed electronically at: *authenticationsummit@ftc.gov*

September 30, 2004

Mr. Donald S. Clark, Secretary
Federal Trade Commission
CAN-SPAM Act
P. O. Box 1030
Merrifield, VA 22116-1030

Re: Email Authentication Summit – Comments (Matter No. P044411)

Dear Mr. Secretary:

TRUSTe is pleased to respond to this request for comments by the Federal Trade Commission ("FTC") and the National Institute of Standards and Technology ("NIST") (collectively, the "Agencies"). We have also submitted a separate request to participate in the related upcoming Email Authentication Summit.

About TRUSTe

TRUSTe is the leading online privacy brand. As an independent, nonprofit organization, TRUSTe is dedicated to enabling individuals and organizations to establish trusting relationships based on respect for personal identity and information in the evolving networked world. Founded in 1997, today TRUSTe runs the largest and award-winning global privacy certification and seal program, with more than 1,500 Web sites certified throughout the world, including those of AOL, Microsoft, IBM, Nationwide and The New York Times. Its seal programs are certified as safe harbors for the Children's Online Privacy Protection Act (COPPA) and the EU Safe Harbor Framework. Information about all TRUSTe programs may be viewed at our web site at http://www.truste.org.

TRUSTe's programs have evolved since its inception to reflect changes in law, technology, industry practices and consumer needs. For example, TRUSTe has introduced Wireless Privacy Principles and Implementation Guidelines. Further, and specific to the issues presented in the announcement of the Email Authentication Summit, TRUSTe has proven expertise in legitimate email and is working on several fronts to further best practices in electronic mail. Our License Agreement now includes program requirements covering Licensees' email practices. TRUSTe also significantly contributes to anti-spam efforts by operating an Independent Trust Authority

("ITA") for email, most specifically as the certification and enforcement authority for Ironport's Bonded Sender program.

For the past 14 months, TRUSTe has taken the lead in solving several key problems in the fight against spam. The current ecosystem of blacklists, content-based spam filters and unmanaged complaint loops has reduced spam, but at a price. TRUSTe has dedicated itself to preserving email as an inexpensive and legitimate means of communication among businesses and consumers, devoid of fraud and spam.

Bonded Sender

TRUSTe's primary effort as an Independent Trust Authority for email is serving as the accreditation and enforcement authority behind IronPort's Bonded Sender. With the successful introduction of the Bonded Sender Program, TRUSTe is now in a unique position as the gold standard of email accreditation authorities. The Bonded Sender Program, for which TRUSTe provides certification, oversight, and dispute resolution services, brings accountability to email with a unique complaint rate enforcement mechanism. TRUSTe certifies participating senders to a baseline set of standards that include consent with robust disclosure and easy unsubscribe tools, as well as technical requirements to ensure that mailers' servers do not assist spammers. Senders must post a significant bond that is debited in the event that consumer complaint rates surpass set thresholds. ISPs participating in Bonded Sender's network agree to deliver email from Bonder Senders, producing increased delivery rates for senders who can maintain low complaint rates.

The Bonded Sender Program was the first of a class of legitimate sender programs and has achieved significant success in its first nine months of operation, amassing over 35,000 receiving networks and more than 100 large senders, including Google, C-Net and About.com. Developing the Bonded Sender Program has required a comprehensive understanding of the dynamics of the current ecosystem and deep knowledge of the full range of existing and emerging technologies aimed at reducing spam.

We also note that TRUSTe offers the valuable and potentially unique perspective of an entity not wedded to any single authentication standard.

Other TRUSTe Efforts in Support of Legitimate Email

TRUSTe is pursuing additional email accreditation strategies and is exploring several key partnerships with leading email technology companies, who look to TRUSTe for guidance and expertise. In its research, TRUSTe has amassed a broad understanding of the full range of available and emerging technologies and standards. TRUSTe is a highly respected contributor to the Anti-Phishing Working Group ("APWG") and the Sender ID Framework initiatives as well.

Further, TRUSTe is uniquely situated to inform the work of the Summit from a consumer perspective. Just yesterday, we announced the results of a national survey of 1,335 U.S. Internet users about phishing, conducted by the Ponemon Institute and sponsored by TRUSTe and the electronic payments association NACHA. Among other insights, the survey reveals that 76 **percent of consumers are experiencing an increase in spoofing and phishing incidents and 35** percent receive fake e-mails at least once a week. Over 64 percent of respondents believe that it is simply <u>unacceptable</u> for organizations to do nothing about spoofing and phishing. About 96 percent of respondents want organizations to consider enabling technologies to help authenticate e-mails and Web sites. We would be pleased to discuss the survey results more fully at the Summit.

Comments in Response to Email Authentication Questions

TRUSTe has chosen to respond only to the specific questions we are able to provide unique or particular insights or information about.

Questions 1 & 25.

The Agencies have asked whether any of the proposed authentication standards (either alone or in conjunction with other existing technologies) would result in a significant decrease in the amount of spam received by consumers, and also whether any of the proposed authentication systems would prevent "phishing," a form of online identity theft. We see these questions as interrelated and accordingly answer them jointly.

<u>Authentication is the first and potentially most important effort to address two of the most critical consumer issues today: Phishing and Spam.</u>

Authentication standards will reduce spam from forged identities -- though significant impact will not be seen until adoption among senders and receivers reaches critical mass. Reductions in spam from authentic senders can only be achieved through supplemental identification, reputation and authentication services. Such services will be more useful once senders can be authenticated.

Domain based authentication solutions assure the receiving network operator that the message is in fact sent by the domain claiming authorship in the message headers. This rudimentary level of authentication is lacking from the SMTP mail infrastructure, which is inherently trusting of mail header information. When a sender sends into a network, the network asks the sender for identification, and the sender passes a value. The receiver has no way to verify the accuracy of that value. Authentication provides the verification, similar to a driver's license, passport, or any other mechanism used offline that provides supporting evidence to an individual's claimed identity. In the case of domain based authentication, only the sender's domain can be validated. The validity of the purported offline identity associated with that domain is not validated by the proposed standards alone.

In general, good domain authentication standards have the power to reduce the volume of spam received by consumers for three reasons:

1. **Spam from forged identities will be blocked.**
   For example, within the current SMTP mail infrastructure, when Illegal Spammer sends mail into Receiving Network, Illegal Spammer can easily claim to be BigAuctionSite.com. Receiving Network can do little to verify Illegal Spammer's claims, unless Illegal Spammer's IP addresses happen to already be blacklisted, either locally or on a public list. The more likely scenario is that Illegal Spammer has compromised vulnerable machines or is sending from new IP addresses, neither of which has yet been associated with Illegal Spammer. When appropriate authentication standards have been widely adopted, Receiving Network will be able to check an authoritative resource (in the case of domain based authentication, a DNS record maintained by the alleged sender) to see if BigAuctionSite.com has truly sent the message. If they have not, the message can be stopped, preferably before it has even entered the network. While many forged identity messages are "phishing" messages (see #2), some forgeries are made simply to gain additional delivery privileges, by either tapping into another entity's positive reputation or by creating an innocuous sounding entity that has no known reputation. In most cases, these messages will be blocked under a domain based authentication system.

2. **Many phishing messages will be blocked.**
   Phishing is arguably the most damaging form of spam. Without describing the typical phishing attempt in detail, it often entails both a forged identity presented to the Receiving Network and consumer-facing visual elements, including branding and URLs that misrepresent the sender's identity to the consumer. Authentication, as currently considered, will have no specific controls on branding within the message body. But at a minimum, Illegal Spammer will not be able to send phishing attacks into Receiving Network while claiming to be BigAuctionSite.com to the Receiving Network. This will be stopped as a case of forged identity, as described above. This alone will reduce phishing attacks as they are performed today. Further, one can easily foresee a time when receiving networks take advantage of the authoritative resources provided by an authentication system to prevent the display of non-authorized URLs that refer to the most frequently phished domains. For example, assuming that Illegal Spammer could get a message through identity-based mail screening tools, their message would be prevented from displaying the URL "billing.BigAuctionSite.com" to consumers, as BigAuctionSite.com would not have this URL listed as authorized in its DNS records (or would have itself – not Illegal Spammer – listed as the owner). Phishing attacks come in many forms, and authentication alone will not end phishing. But it will immediately eliminate forged identity phishing, which will force spammers to use more creative, and hence less convincing, identities (for example, support@newspammydomain.BigAuctionSite3.com, instead of support@BigAuctionSite.com), and it will facilitate the development of more advanced anti-phishing techniques.

3. **A platform for additional mail screening inputs.**

> Authentication in itself provides only the most basic information for the mail screening decisions of receiving networks. While authentication alone will likely have a positive impact on the volume of spam email consumers receive, the greater impact will occur when this platform is extended to facilitate a range of reputation and accreditation services (more on this below). These services are not useful when receiving networks are unable to authenticate the sender, as further information on mailing history and principles is unreliable in such an environment. Using this information together, receiving networks will be able to greatly reduce the volume of spam that consumers receive from both forged and non-forged sources.

While TRUSTe believes that authentication standards will reduce the volume of spam consumers receive and their susceptibility to phishing scams, the short-term impact on volume may not be immediately evident in spam volume statistics until additional programs leveraging the authentication are further developed and deployed. In particular:

1. **More than one protocol is likely to emerge, leading to "wait and see" implementations.**
   Several major players have aligned themselves behind competing authentication solutions (Sender ID, SPF, Domain Keys, and CSV/BATV). Each proposed solution has independent strengths and weaknesses, which could lead to individuals and organizations choosing solutions that meet specific requirements for completeness versus ease of implementation. Presented with such choices, some senders will wait on the sidelines to see if one or several emerge as the most feasible for their peers. In addition, many of those that have already positioned themselves behind a specific authentication standard now have an entrenched political interest in seeing one emerge over the others. This can lead to factionalism, and may further delay adoption.

2. **The agreed upon protocol(s) will not be adopted by all parties immediately.**
   Once industry agrees upon one or several authentication standards, the adoption curve begins. Major ISPs will likely adopt the standards quickly, and MTA packages, both proprietary and open source, will include the standards in short order. SendMail, for example, has already released a Sender ID plug-in. But small to medium sized enterprises will take anywhere from two to 24 months to update their MTA software, and in the meantime a substantial portion of the Internet will not be set up to use the authentication standards. Adoption in the sender community will be similarly segmented, but will likely focus on those that are simplest to implement in the short term, such as Sender ID, which requires only a simple change to the sending domain's DNS record.

3. **Authentication results will prompt "soft" decisions until adoption is widespread.**
   Receiving networks will not reject outright email that lacks proper authentication until the protocol is widely adopted, for fear of rejecting mail that consumers want to receive from well-intentioned senders on the tail end of the adoption curve. Late adopting senders will not have great incentive to authenticate their mail until receiving networks begin making "hard" rejections. After a certain period of fair warning, the major ISPs are likely to go ahead and begin rejecting mail from unauthenticated senders, which will prompt the late adopters to comply. But this process will create a built-in lag time between the point of first industry declaration and actual impact on spam volume that could last six to twelve months.

Senders and receivers will consider many nuanced criteria in making decisions about which authentication protocols to implement, such as ease and expense of implementation, impact on throughput, reliability and long term viability. For example, certain standards provide no protection against a combination of spoofed domain and IP address, or against phantom domains which were acquired using a false identity.

__Question 6.__ The Agencies have asked whether the authentication standards are mutually exclusive or interoperable, and whether any of the proposed authentication standards would integrate with any other standards. For example, if Mail Server A is using standard X, will it accept email easily from Mail Server B that is using standard Y?

In general, the major authentication standards can be implemented concurrently. Receiving networks are likely to implement checks against all the authentication standards that both (a) gain wide adoption, and (b) provide useful information, beginning with the least resource intensive and continuing to the most. By way of example, if both Sender ID, which Microsoft still intends to deploy, and DomainKeys, supported by Yahoo and now AOL, gain adoption, receiving networks may implement the following sequence of checks:

1. (Sender ID) Using the "sender optimization" feature of Sender ID, receiver checks the "Submitter" domain against the corresponding SPF record. This check ensures that the last network hop was accurately reported and is done before the full message is downloaded.
    - If no Submitter tag, skip this check
    - If sender fails, reject message
    - If message passes check, download message and continue with test 2 ...

2. (Sender ID) The receiver checks the "Purported Responsible Address" after the message is downloaded against the corresponding SPF record.
    - If no Sender ID DNS record, skip this check
    - If sender fails, delete message
    - If message passes check, continue ...

3. (DomainKeys) Extract header based signature and From: domain. Check private key against public key presented in From: domain DNS entry. This provides a check for the original sender (not just the last hop) and ensures that the message has not been altered during transit.
    - If no public key, skip this check
    - If sender fails, delete message
    - If message passes check, continue

4. (No authentication available) Once the above checks are completed and no authentication method was found, warn the user or delete the message based on receiver's local policy.

With this implementation (or a similar one), a message should be processed successfully whether or not a sender is compliant with either one or both Sender-ID and DomainKeys, and messages lacking authentication data can either be deleted or presented to recipients with a warning.

__Question 7.__ The Agencies have asked whether any of the proposed authentication standards would have to be an open standard (i.e., a standard with specifications that are public).

The proposed authentication standards must be open if they hope to gain wide adoption. In recognition of this, the leading standards under consideration have all taken great pains to subject themselves to standards body analysis (Sender-ID, Domain Keys, CSV). Any standard that wishes to remain proprietary will be ignored by the open source MTA packages and will find it virtually impossible to be adopted by the major ISPs, most of whom have already taken a public position with one or more open authentication solutions. These rollout challenges, plus additional cost burdens on senders, will retard sender adoption, further limiting private ecosystem usefulness unless significant additional value can be offered to senders and receivers alike.

__Question 29.__ The Agencies have requested a description of how the Email Authentication Summit can support industry or standard-setting efforts.

By providing an arena for open discussion and expert testimony, the Summit could help to clarify the potential and need for open authentication standards and bring transparency and alignment to the respective strengths and weaknesses of each proposed standard. TRUSTe hopes that the Summit will attract a full range of solution providers, email senders and both large and small receiving networks, thus providing a chance to improve industry cooperation and alignment -- which is necessary to provide long term relief from fraudulent and spam abuse of the email infrastructure. As a purely digital medium, the internet has the potential to provide the most secure means of communication in human history, but this can only be accomplished with a common vision and mutual will. We hope the Summit will inform industry participants, establish basic goals, and start to identify additional implementation measures to achieve those goals.

__Question 30.__ Assuming a domain-level authentication system is established in the near term, the Agencies have requested a description of future measures that the private market should develop and implement in order to combat spam.

Authentication is widely considered to be the first in a series of steps that industry must take to provide receiving networks with the information they need to effectively block all types of spam from recipients' inboxes. The Email Service Providers Coalition has presented one of the more developed models using this structure in the Project Lumos White Paper. When reputation and accreditation data are added to authenticated email, a substantial reduction of spam volume from non-forged senders becomes possible. However, each solution needs to be assessed for future vulnerabilities. Creative spammers will invent new techniques, such as IP spoofing, phantom domains and others, because the economic incentives are very high.

TRUSTe would describe each of these components as follows:

- **Authentication**: A validated connection between the sending IP address and the domain asserted as the sending domain. (Non-IP systems are also in discussion.) This can be enhanced with a connection between domain and physical entity, a la Verisign's validated domains list.

- **Reputation**: Numeric scoring of sender quality using historic data such as mail volume, complaint rate, abuse history, quality of DNS records, list hygiene, etc. Advantages: reacts quickly to behavioral changes, and data will be available on all senders, not just manually reviewed senders. Disadvantages: much more helpful in identifying black hat spammers. Within grey areas, score can be a poor accounting and often misses critical factors like legal compliance, third party sharing, natural variations across business types, etc. Cripples well-intentioned companies that would like to improve. New companies will have no reputation.

- **Accreditation**: Thorough review of sender's compliance with a transparent set of email standards. Standards would include permission level, quality of consumer disclosures, sharing practices, etc. Senders can self-accredit, volunteering their standards in a public record according to a commonly accepted format, or they can be accredited by an independent third party, which offers obvious credibility advantages. Third parties would provide ongoing monitoring and enforcement to ensure continued compliance over time and dispute resolution services to provide program accountability.

These three sets of information provide a receiving network with the following information:

1. I know who the sender really is
2. The sender does not have an egregious sending history
3. The sender abides by a set of business practices consistent with the law and the reasonable expectations of the email consumers on my network

In keeping with this framework, the leading authentication standards have been designed such that they provide an excellent technological platform to make additional statements, particularly about the sender's email policy and their status with accreditation authorities. Sender ID requires the sender to publish an SPF record in their DNS. This record can easily be extended. DomainKeys requires the sender to publish a pubic key in the DNS. With receivers checking this record for key matches, it again provides a logical point of extension. The internet drafts for both specifications refer explicitly to the role of authentication not as a stand alone cure for spam, but as a cure for forged identity email and a foundation for the additional data points that receiving networks require to effectively combat spam.

We note, finally, that regardless of how authentication systems such as those described above may develop in the future, TRUSTe continues to believe that there will always be an important role for self-regulatory, third-party certification programs as a complementary approach to fighting spam. We point to the example of IronPort's Bonded Sender Program, as described earlier in this letter.

In closing, we wish to thank the Agencies for this chance to share TRUSTe's perspective on these issues, and for the potential opportunity to provide further insights at the upcoming Email Authentication Summit. In the meantime, we would be happy to discuss these issues further or respond to any questions you may have.

For further information, please contact: Fran Maier, Executive Director & CEO, at 415-520-3418, email: fmaier@truste.org; David Currie, Vice President of Business Development, at 415-520-3401, email dcurrie@truste.org; or Colin O'Malley, Director of Product Development, at 415-520-3408, email comalley@truste.org.