COMMENT ON EMAIL AUTHENTICATION SUMMIT ISSUES

AGENCY: Federal Trade Commission ("FTC" or the "Commission")

This comment is submitted by the Council of American Survey Research Organizations, Inc. ("CASRO") in response to the Commission's Notice announcing that an Email Authentication Summit has been scheduled for November 9-10, 2004, and requesting comments on issues related to email authentication.

CASRO is a not-for-profit industry and professional association representing nearly 250 research companies and institutions engaged in survey research regarding a wide variety of public policy, forensic, health, scientific, economic and other public and private areas of inquiry. Its members are responsible for the overwhelming majority of the survey research conducted each year in the United States and a major portion of global survey research.

Survey research contributes significantly to the public interest by providing reliable, verifiable analyses of a wide variety of public policy, sociological, legislative, regulatory, political, forensic, scientific, public health and economic areas of inquiry. Survey research is an invaluable and irreplaceable tool of behavioral science used to measure, track, analyze and predict public attitudes, opinions, awareness and preferences. Survey research is virtually the only source of statistically reliable and verifiable information of this type, on which government, business and private interests rely to formulate their actions and decisions.

Among the principal missions of CASRO is the establishment, maintenance and enforcement of professional and ethical standards in survey research and the protection of the privacy interests of those who participate in survey research. These principles reflect the social utility of survey research and the need to protect and respect the industry's most valuable resource -- its survey respondents.

As one of the leading representatives of the U.S. survey research industry, CASRO has an interest in articulating the compelling public, governmental and business need for protecting not only survey research, but also the rights and concerns of the public and survey respondents. We believe that privacy is one of these important concerns. Accordingly, CASRO supports the Commission's actions in protecting consumers' right to privacy.

In furtherance of this goal of protecting consumers' privacy interest, CASRO supports the FTC and the National Institute of Standards and Technology ("NIST") in their decision to host an Email Authentication Summit (the "Summit") on November 9-10, 2004.

One of the greatest hurdles facing the survey research industry today is the practice of emailers concealing their true commercial purpose by posing as survey researchers. This practice, known as "sugging" or "selling under the guise of research" involves marketers masking their solicitations or advertisements as invitations to participate in surveys. This practice has dissuaded potential survey respondents from participating in surveys for fear that they will become the targets of unsolicited email marketing, The Commission already explicitly prohibits sugging by telemarketers as a deceptive trade practice.

The current "open" nature of email technology , together with the lack of a uniform email authentication system contribute to the grave difficulties that regulators face in trying to curb sugging and other forms of spam. CASRO therefore supports the efforts of the Commission to offer a practical solution under the CAN-SPAM Act to alleviate this problem.

In connection with its planned Email Authentication Summit, the Commission has requested answers to thirty specific questions. CASRO respectfully offers the following in response to that request:

Question 1. 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.

Answer: We believe that instituting a domain-level authentication standard would result in a significant decrease in the amount of spam received by consumers.

Question 2. Whether any of the proposed authentication standards would require modification of the current Internet protocols and whether any such modification would be technologically and practically feasible.

Answer: We believe that all of the current authentication standards would require revisions to the current Internet protocols; however, we feel that these revisions would be both technologically and practically feasible.

Question 3. Whether any of the proposed authentication standards would function with the software and hardware currently used by senders and recipients of email and operators of sending and receiving email servers. If not, what additional software or hardware would the sender and recipient need, how much it would cost, whether it would be required or optional, and where it would be obtained.

Answer: Existing mail servers and client servers will have to be enhanced to support the proposed standards. This enhanced software would be obtained from the software vendor that supplied the current software. The new standards should not impact hardware for end users, but could result in hardware upgrades for ISPs, etc.

Question 4. How operators of receiving email servers are likely to handle unauthenticated messages.

Answer: Operators of receiving email servers are likely to discard unauthenticated messages.

Question 5. Whether any of the proposed authentication standards could result in email being incorrectly labeled as authenticated or unauthenticated (false negatives and false positives), and the steps that could be taken to limit such occurrences.

Answer: It is possible that there could be false negatives and positives as a result of any authentication standard. The most logical method for limiting such occurrences would be to examine the circumstances surrounding the false positives and false negatives and implement fixes during a phased in de-bugging period.

Question 6. Whether the authentication standards are mutually exclusive or interoperable. 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?

Answer: The authentication standards will most likely be vendor dependent, as a result, interoperability might have to be achieved over time after the standards are implemented. The key to achieving this interoperability is the application of open standards.

Question 7. Whether any of the proposed authentication standards would have to be an open standard (i.e., a standard with specifications that are public).

Answer: We believe that the standards adopted should be open standards.

Question 8. Whether any of the proposed authentication standards are proprietary and/or patented.

Answer: It is unknown at this point whether any of the proposed authentication standards are proprietary or patented.

Question 9. Whether any of the proposed authentication standards would require the use of goods or services protected by intellectual property laws.

Answer: It is a possibility that some of the proposed authentication standards would require the use of protected goods or services.

Question 10. How any of the proposed authentication standards would treat email forwarding services.

Answer: We believe that all of the proposed authentication standards would treat email that has been sent through a forwarding service in the same manner as any other message.

Question 11. Whether any of the proposed authentication standards would have any implications for mobile users (e.g., users who may be using a laptop computer, an email-enabled mobile phone, or other devices, and who legitimately send email from email addresses that are not administratively connected with their home domain).

Answer: The adoption of an email authentication standard should have no discernable implications for consumers sending messages through mobile devices.

Question 12. Whether any of the proposed authentication standards would have any implications for roving users (i.e., users who are obliged to use a third-party submission service when unable to connect to their own submission service).

Answer: The proposed authentication standards could impact roving users who are obligated to use a third party submission service when unable to connect to their own submission service because in that situation, the domain might not match up to the IP address, preventing the message from being authenticated.

Question 13. Whether any of the proposed authentication standards would affect the use of mailing lists.

Answer: None of the proposed authentication standards should affect the use of mailing lists as the mail servers associated with these lists should have their own IP addresses, and should therefore be easily authenticated.

Question 14. Whether any of the proposed authentication standards would have any implications for outsourced email services.

Answer: Provided that the DNS of the outsourced email service is properly configured, the institution of an authentication standard should not affect these services.

Question 15. Whether any of the proposed authentication standards would have an impact on multiple apparent responsible identities (e.g., in cases where users send email using their Internet Service Provider's SMTP network but have their primary email account elsewhere).

Answer: We believe that in such a situation, the authentication standard should not impact whether the message is authenticated. However, if the user's email address is not configured properly to allow for such activity , the email message may not be authenticated.

Question 16. Whether any of the proposed authentication standards would have an impact on web-generated email.

Answer: We do not believe that any of the authentication standards would have any impact on web-generated email.

Question 17. Whether the proposed authentication standards are scalable. Whether the standards are computationally difficult such that scaling over a certain limit becomes technologically impractical. Whether the standards are monetarily expensive due to hardware and resource issues so that scaling over a certain limit becomes impractical.

Answer: Answers to all of these issues would depend upon the standard that is implemented.

Question 18. Identify any costs that would arise as a result of implementing any of the proposed authentication standards, and identify who most likely would bear these costs (e.g., large ISPs, small ISPs, consumers, or email marketers).

Answer: Upgrades to email server hardware would probably be required. Bandwidth shouldn't be impacted as unsolicited email should decline. Costs would be carried by ISPs, etc., but may be offset in reduction in costs associated with spam remediation.

Question 19. Whether ISPs that do not participate in an authentication regime would face any challenges providing email services. If so, what types of challenges these ISPs would face and whether these challenges would in any way prevent them from continuing to be able to provide email services.

Answer: An ISP that chooses not to participate in an authentication regime might not be able to provide viable email services to consumers.

Question 20. Whether an Internet-wide authentication system could be adopted within a reasonable amount of time. Description of industry and standard setting efforts, whether there is an implementation schedule in place and, if so, the time frames of the implementation schedule.

Answer: The industry should take action to ensure open standards for the authentication standard that is implemented. Optimistically, any authentication standard would take six to twelve months to develop, and another six to twelve months to implement. Again, we believe that open standards should be pursued.

Question 21. Whether any of the authentication standards would delay current email transmission times, burden current computer mechanisms, or otherwise adversely affect the ease of email use by consumers.

Answer: Any authentication standard could delay the transmission time of email or burden computer mechanisms if ISPs fail to make the hardware and software upgrades necessary to ensure the smooth implementation of the authentication standard.

Question 22. Whether any of the proposed authentication standards would impact the ability of consumers to engage in anonymous political speech.

Answer: It is possible that the proposed authentication standard could impact the ability of consumers to engage in anonymous speech in that it could become very easy to trace the domain source of an email message. However, authenticating the domain from which an email comes from does not verify the specific address within the domain that generated the message, so the ability for a consumer to remain anonymous could be maintained .

Question 23. Whether any safeguards are necessary to ensure that the adoption of an industry-wide authentication standard does not run afoul of the antitrust laws.

Answer: The easiest and most logical safeguard that the industry could adopt would be the guarantee of open standards with respect to the authentication system.

Question 24. Whether a spammer or hacker could compromise any of the proposed authentication standards by using, for example, zombie drones, spoofing of originating IP addresses, misuse of public/private key cryptography, or other means.

Answer: We believe that the possibility will still exist that a spammer or hacker could compromise the proposed authentication standards, however, this risk should not discourage the implementation of any of the standards.

Question 25. Whether any of the proposed authentication systems would prevent ‘‘phishing,’’ a form of online identity theft.

Answer: We do not believe that any of the proposed authentications will prevent phishing.

Question 26. Whether the operators of small ISPs and business owners would have the technical capacity to use any of the proposed authentication standards. Whether any of the authentication standards could be reasonably implemented by smaller ISPs.

Answer: Small ISPs and business owners would have the technical capacity to use all of the proposed authentication standards. Whether the ISPs and business owners choose to bear effort and the expense to upgrade their hardware and software as needed to implement the standard would be a business decision on their part.

Question 27. Whether any of the proposed authentication standards would have cross-border implications.

Answer: We believe that the authentication standards could have cross-border implications, and as a result, global issues should be considered when determining which authentication standard will be implemented.

Question 28. Whether any of the proposed authentication standards would require an international civil cryptographic standard or other internationally adopted standard and, if so, the implications of this requirement.

Answer: We do not believe that an international civil cryptographic or other international standard would be required by any of the authentication standards.

Question 29. Description of how the Email Authentication Summit can support industry or standard-setting efforts.

Answer: We believe that the most effective way for the Email Authentication Summit to support standard setting efforts is to recommend a competent standards group to pursue an open standard.

Question 30. Assuming a domain-level authentication system is established in the near term, future measures that the private market should develop and implement in order to combat spam.

Answer: In the future, the industry should require that all Internet edge routers verify incoming networks to prevent Denial of Service Attacks and IP Spoofing.