



**Deborah Zuccarini**  
**President**

Experian Marketing  
Solutions  
955 American Lane  
Schaumburg, IL 60173  
(224) 698-8409

September 30, 2004

Mr. Donald S. Clark  
Secretary  
Federal Trade Commission  
Room 159 – H (Annex V)  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

Re: Email Authentication Summit – Comments (Matter Number P044411)

Dear Mr. Secretary:

Experian and its email service provider (ESP) subsidiary, CheetahMail, appreciate having the opportunity to comment on email authentication pursuant to the Commission's and the National Institute of Standards and Technology's request for comments issued on September 15, 2004. Enclosed is the response of Experian and CheetahMail to the 30 questions posed by the Commission and NIST.

Experian has vital interests in these discussions because of our roles as a large-volume email services provider (ESP), as a major sender of email, and as a national consumer reporting agency. In a separate communication, Mr. Frederick Lindberg, Chief Technology Officer for Experian/CheetahMail, is submitting a request to participate in the November 9-10 Authentication Summit. We would hope that the Commission and its staff would use us as a resource going forward.

Sincerely,

A handwritten signature in black ink that reads "Deb Zuccarini". The signature is written in a cursive, flowing style.

Deborah Zuccarini  
President, Marketing Services

Enclosure

**Email Authentication Summit  
Comments of Experian/CheetahMail to Questions  
Raised by the Federal Trade Commission  
(Matter Number P044411)**

***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.***

Quantifying the reduction in spam is first dependent on a common definition of spam. There are two common definitional categories; a) email which is fraudulent as defined by the CAN SPAM Act, and b) bulk unsolicited commercial email, which many consumers believe to be spam and, as a result, base many of their “spam” complaints to their respective ISP’s.

With respect to category (a), it is our belief that a significant portion of fraudulently sent email through traditional routing mechanisms can be eliminated through authentication. Since most of these spammers are abusing the Internet’s open architecture, only those that truly show their “connection” to the Internet community will continue to operate. While it is difficult to quantify an accurate percentage of unauthenticated email which will be filtered as spam, as each receiver treats messaging differently, it is clear that the great majority of spam is currently unauthenticated and will be more easily separated from legitimate inbound messaging and identified as fraudulent. This elimination also does not take into account “zombie” email hijacking, which uses an account of an existing broadband user to send spam and will be viewed as authenticated.

However, category (b) is an entirely different matter. We believe that many of the spammers in category (a) will migrate to category (b) and truly “connect” to the Internet community and continue their operations. As we have witnessed in the early stages of authentication compliance, many spammers and bulk unsolicited commercial emailers have purchased what can commonly be called “disposable domain names” and use these in conjunction with any number of Internet Protocol (IP) addresses they receive from ISP’s all over the world. Since it is extremely easy to purchase inexpensive domain names and create or switch ISP’s, these more endowed and resourceful spammers can effectively continue their operations.

This advanced requirement for spammers and bulk unsolicited commercial emailers to continually migrate through domain name and IP changes will force many of the less endowed or resourceful fraudulent or deceptive emailers out of business. That said, only a minority of spam in category (b) will automatically be eliminated through authentication.

As a result, spam will be effectively decreased. However, if a definition of “significant” is much more than 50%, we are unsure whether this can be achieved under the more commonly implemented “single level” domain authentication framework.

This estimate does not take into account a combination of current authentication proposals with other advanced anti-spam proposals, such as cryptography, Bayesian filters, peer-to-peer filtering networks, challenge-response systems, and accreditation and reputation systems. On a number of levels, we believe, spam can be effectively eliminated if authentication is combined with some of these additional elements.

***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.***

The current authentication standards proposals do not require any true modification to the current Internet protocols. Changes only need to be made to connected software and domain name system records that indicate whether the connected computing systems are accurate.

However, even with email authentication standards, there are still openings within the Internet protocol system for exploitation by spammers. For example, it is impossible to determine any information verifying the receipt and use of IP addresses across the Internet. Because the Internet Assigned Numbers Authority has never been accountable for allocation of these addresses, the many millions of exchanges that enable anyone to connect to the Internet remain mostly anonymous. With the new IPv6 system being introduced, this process will only enable further anonymity. If an authentication standard were to be 100% effective, it would require significant changes to Internet Protocol address allocation. In addition to IP address allocation, there needs to be careful review of the process of domain name registration. It is remarkably easy for any consumer or business to purchase domain names that can be used for spam and phishing, and connect them to any IP address in the world that could host such fraudulent operations. If spam and phishing are to be eliminated, this process needs further authentication and verification procedures in place to discourage fraudulent uses of the Internet.

***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.***

Most email senders and receivers will need to update their software, not hardware, to reflect changes with authentication. The majority of these updates will not require any additional software, but rather updates from their existing software providers or updates built by an internal administrator.

Because there is not one common standard being endorsed by the Internet standards-setting bodies, both senders and receivers will need to determine a scope of changes to their systems, which will have some cost, with updates and maintenance. Even though these changes are entirely optional, with enhanced scrutiny for un-authenticated email,

senders will have little choice but to authenticate with any and all authentication proposals. Finally, these changes will also require senders to continually monitor how varying receivers are treating their authentication records, thus requiring some additional labor and technical costs with compliance. Since there is no common standard for email receivers to notify senders if authentication records are inaccurate, then the onus is on email senders to continually monitor receipt of email with receivers, and note any negative trends that take place with their authenticated messaging. This process of monitoring is not trivial, and will require some significant labor resources to ensure that all authenticated messaging is being treated similarly across major receivers.

#### ***4. How operators of receiving email servers are likely to handle un-authenticated messages.***

This question (and the following questions related to it) is perhaps the most important of all of the inquiries surrounding email authentication, not just for the question of un-authenticated messages, but also for inaccurately authenticated messages. In the many years Experian/CheetahMail has been an email service provider for volume senders, we have witnessed an incredible variety of anti-spam initiatives that receivers have implemented. Those initiatives have resulted in erroneous filtering of permission-based email, resulting in “false positives.”

For our purposes, we would like to rephrase the question to ask; “How will receivers handle un-authenticated email or inaccurately published authentication records?” Since both are most likely in the same category, some spammers will undoubtedly falsely attempt to authenticate their messages and fail. Under this scenario, and in one such authentication proposal, a receiver is expected to reply to the sender with a particular bounce-error code indicating that the message is either un-authenticated or inaccurately authenticated. Unfortunately, the proposed bounce error code system, as proposed in RFC 1893 (<http://www.faqs.org/rfcs/rfc1893.html>) has been ignored or abused by some receivers in efforts to further deny spammers information about recipients. Unfortunately, this practice also significantly impacts the legitimate processing of error-laden email by senders.

We request that all receivers cooperate with RFC 1893, and reply to unauthenticated or inaccurate authentication records with accurate bounce-reply codes, such as 5.7.7. This code communicates that a receiver believes that an email has violated its acceptable use policy and should not be resent unless that policy is addressed. If the correct error codes were applied – perhaps with a unique 5.7.7 code - to authenticated messages, then legitimate senders could either investigate their mistake or contact the receiver for more information. This corrective action is noteworthy, since spammers ignore these error codes and would not make the effort to re-send to a permanent failed bounced address.

#### ***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.***

