Comment #: 33

experian

**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,

Deb Zuccarini

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.*

As mentioned earlier, the issue that most concerns Experian/CheetahMail is whether inaccurately authenticated mail could be filtered as spam, or whether it could be responded to with an error code that indicates a minor inaccuracy that could be resolved. This false positive problem will escalate from currently manageable proportions to more significant levels if numerous receivers are implementing varying degrees of authentication and are not replying to senders with accurate mailbox error codes.

Finally, we are also concerned that "zombie" (referenced earlier) spam will also be viewed as authenticated, and thus further reduce the effectiveness of these proposals.

To restate the position of Experian/CheetahMail, the implementation of sender authentication must hinge on the two factors. First, receivers must agree to implement accurate RFC 1893 error codes. Second, receivers must respond to inaccurate authentication records with a designated authentication-related or other policy-related code, such as 5.7.7.

***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?***

Regarding obligations for senders, experiences with the first stages of authentication suggest that it is complimentary to authenticate if a sender is implementing multiple standards.

However, with receivers; there are two answers:

a. A receiver could be checking "single" level domain authentication with the reply-to/return-path address.
b. A receiver could be checking "dual" level domain authentication to both the visible "from" field and the reply-to/return-path address.

In the case of (a), it is seemingly compatible that a sender publishing single or dual records would be authenticated.

As a result of item (b), it is unclear how receivers who are checking the dual level of authentication would treat incomplete or single records. It is a possibility that this mail will not be considered authenticated. Therefore, inaccurate or incomplete authentication by legitimate senders could be labeled or filtered as spam.

For example, it has come to our attention that one major receiver has plans to accept all incoming mail, authenticated or otherwise, based on the dual authentication proposal, and visibly inform their recipients in their client interface whether the mail is authenticated or not. The result of this "unauthenticated" visible labeling, even if the sender is using an alternative authentication proposal, could be detrimental to a sender's brand and recipient loyalty. If many legitimate senders are appearing to be unauthenticated this could also have an unfortunate result of raising doubts about the security and effectiveness as email as a medium.

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

Standards are inherently public and open. If it is not public, it is a proprietary solution. In order for authentication to be a commonly implemented, it will need to be an open and public standard. Otherwise the proposed standards will be in the same capacity as current anti-spam efforts and lead to fragmentation and competitive positioning. As the current anti-spam market is already highly competitive, fragmented authentication processes will only further make volume email sending more difficult as each major receiver filtering system requires continual monitoring to ensure against false positives.

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

A number of organizations have applied for patents for authentication protocols. It is unclear what the ramifications of these patents would have on sender and receiver usage. It would be very helpful for the FTC to coordinate with the USPTO to highlight and determine the impact of such applications on email authentication implementation.

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

The unclear patent applications make it difficult for Experian/CheetahMail to answer this question with confidence.

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

There are a number of forms of email forwarding services affected by varying degrees of authentication. There are services that forward email based on an "alias" from one address to another. There are also forwarding services with primarily commercial applications that enable individuals to use the web to forward messages conveying a published article or relevant commercial email or web page. We will address the latter service because Experian/CheetahMail offers such forwarding service as part of our product features.

As addressed in our responses to the FTC's Advanced Notice for Public Rulemaking (ANPR) regarding the CAN SPAM Act, it is difficult for companies engaged in email and online services to clearly identify compliance with respect to email forwarding, or "refer-a-friend" services. Both the initiator and entity responsible for the commercial content being forwarded must comply with the CAN SPAM Act and appropriately convey, label and offer an unsubscribe option. As stated in our ANPR response, it is very difficult for companies to comply with these requirements, as it is the position of the companies offering the content for forwarding that these emails are being sent only by the initiator and not a commercial entity on behalf of the initiator. In order to comply, both parties need to offer and honor unsubscribe requests, which is an expensive and confusing proposition for all parties involved.

This problem directly applies directly to email authentication. Experian/CheetahMail's forwarding service enables the initiator to send the message on behalf of itself, clearly labeling the "from" field as that initiator. This results in the recipient not being confused about what messages are being sent by a commercial entity rather than a friend. Under one authentication proposal, it would be impossible to authenticate the initiator because our sending servers can not currently verify the authenticity of the initiator. With another proposal, we can verify our authenticity and showcase this with the identification of an "on behalf of" statement. This statement demonstrates that we are attesting for that initiator, even though it is extremely difficult, in fact, to actually attest for that authenticity as most of the initiators of these messages can easily "spoof" such addresses. As all of our forwarding services are web-based to begin with, authenticating these initiator addresses would require another level of technical verification, which may or may not be easy or cost effective to implement.

To summarize, we believe that there is not yet a clear direction for email forwarding authentication and that the Internet standards-setting bodies should take a closer look at endorsing one or more applications that would gain critical mass in authenticating these services. More importantly, we ask that the FTC respond to our ANPR and NPR request to clarify compliance with the CAN SPAM Act as it relates to forwarding services. This clarity could help us identify which party is responsible for the "from" address and would require additional levels of authentication.

***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).***

No comment.

***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).***

No comment

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

Assuming this question regards automated discussion lists, the response may be viewed similarly to our answer to question # 10 regarding "forwarding services."

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

As a large email service provider, Experian/CheetahMail is witnessing a number of implications with email authentication. In addition to the error-code, false-positive, and forwarding services issues, we can elaborate on three other key issues related to domain-level authentication.

The first issue is the use of a **common domain name** with outsourced email services. In general, email sender domain name owners are required to publish authentication records indicating exactly which sending servers are allowed to reference that domain. As a result, there are multiple first and third party entities sending email on behalf of a single domain owner. Therefore, these authentication records need to be entirely accurate, and continuously updated to reflect exactly which sending servers are operating on their behalf. Since ESPs operate a large number of servers on behalf of clients, they must reference all of these servers or dedicate specific IP resources to these clients. This necessity leaves tremendous room for error in continually referencing and updating these servers. With dedicated IP resources, clients will most likely incur additional fees, which is often a burden to implementation. In both cases, there are added responsibilities for technical operators at a client-sender company, which will result in additional costs in email maintenance. As additional domain authentication proposals are implemented, the difficulty addressing these updates will be compounded, further increasing costs to senders.

The second issue is the use of an **allocated sender subdomain** for outsourced email services. This enables the sender to split their domain from a common domain such as "example.com," to a subdomain such as "e.example.com." Either the sender or the ESP can administer the "e.example.com" subdomain. In either case, the authentication records need to indicate the servers of the ESP. The same authentication situations apply to subdomain allocation as they do with common domain usage. However, in a number of instances, it has been apparent that companies using multiple subdomains with multiple outsourced providers do not necessarily know exactly which subdomains are used for which purposes. Some may only be used as a "reply-to/return-path" functionality, whereas others are used as the "from" or "mail from" address itself. ESPs and/or senders must account for each of these uses since each unique authentication proposal will look to each of these addresses for complete authentication. The burden is then placed on both the sender and the ESP to ensure that each use of these subdomains has accurate authentication records, since one mistake could impact each of the users of that subdomain.

The third issue is with the use of the **ESP domain**, rather than use of the senders'. This issue has little to do with authentication itself, since the ESP will handle that portion relatively easily, but rather with the recipient impression of that use of an ESP domain. As a result of the relationship between phishing and spam, many recipients are wary of any domain use that is not entirely representative of the sender. While it is a goal of the ESP to reference a senders' domain or subdomain, time and cost constraints often result in ESPs using their domain name instead. Therefore, even though a receiver may authenticate an ESP's domain, it is imperative that the FTC and the industry help educate recipients that use of an alternative domain is an acceptable practice. This education would help ensure that recipients do not consider the email to be a phishing attack or spam as a result.

***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).***

No comment

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

No comment

***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.***

Scalability of domain-based authentication is not an apparent problem for senders. Scalability of cryptography-based solutions may require additional computer processing power and potential hardware upgrades.

***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).***

Each participant in authentication, with the exception of the recipient, bears a cost with this process. The senders require significant labor costs in identifying their internal and external sending servers. ESPs require some software costs and significant labor costs in monitoring and ensuring accuracy with authentication references. Both senders and ESP's also bear significant costs in determining and meeting CAN SPAM Act authentication compliance requirements, such as those surrounding forwarding services and combined with the continuing uncertainty surrounding the definition of "sender" with multiple advertiser email messages.

As mentioned earlier, fragmented and multiple variations of authentication will lead to significant increases in time commitments and costs.

***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.***

No comment

***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.***

As of the date of this response, it appears that such an "Internet-wide" common approach to authentication is not possible. The proposed domain-based authentication standards have been negated by dissention amongst the industry on how to treat certain intellectual property requirements. There appears to be no schedule for re-engaging a discussion of an alternative commonly agreed upon domain-based proposal, bur rather efforts are underway to consider multiple domain-based options layered with cryptography and accreditation/reputation services.

For reasons stated previously, this fragmentation of domain-based authentication will continue to be a problem for all parties. Further, it may potentially limit both the effectiveness of overall spam reduction and efforts aimed at reducing phishing.

***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.***

As mentioned earlier, there are some ISP's that have plans to deliver all unauthenticated or inaccurately authenticated email and notify recipients of that information. Since consumers are already wary of spam and phishing, a reference to a legitimate email being unauthenticated may very well mistakenly correlate that message with fraud. It would be a great disservice to consumers if legitimate emailers were mistakenly considered spammers or phishers.

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

No comment

***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.***

No comment.

***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.***

The current environment, where dual authentication proposals are being considered will limit the ability for spammers or hackers to accurately "spoof" a reputable sender domain name. The exception is with spoofing of ISP domain names within their own network. This may be a continued problem for ISP's, that will require cryptography and other solutions to resolve.

However, this does not take into account the ease of registering similar domain names to those of legitimate businesses and effectively "spoofing" that company's brand in an email message.

***25. Whether any of the proposed authentication systems would prevent "phishing," a form of online identity theft.***

Only one of the proposed authentication systems prevents phishing by referencing the dual levels of "from" addresses of the sender. However, the more commonly implemented authentication system only references the initiator "mail from" address, thus limiting the effectiveness against phishers who fraudulently reference the sender's domain name in the visible "from" address.

Unfortunately, the dual level authentication system referenced is laden with potential intellectual property questions, forcing many industry implementers to not pursue this solution.

Experian is not only an ESP servicing many financial services and other "account-based" interests but also is a credit reporting agency. Therefore, it is in Experian's interests to see a widespread dual-level authentication system adopted to help combat phishing. Any proposals or means to accomplish this goal are our utmost priority.

***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.***

No comment

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

Internet standards are cross-border and there should be no reason why international interests can not adopt the same authentication systems.

***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.***

No comment

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

A summit of all respective large implementers of authentication systems can work toward these key goals. The first goal is resolving technical disputes across implementers of various authentication systems. Operability and transparency across implementation is critical and competitive advantages should be set aside. These issues include the resolution of the RFC 1893 error code usage and the question of standard receiver-side authentication inaccuracy reporting.

The second goal is resolving some of the concerns with implementing a complete set of authentication solutions that would address phishing issues. If most receivers only implement a single level "mail from" authentication solution, then spammers and phishers can continue to forge any legitimate brand domain they wish in the visible "from" field. The issue of intellectual property restrictions needs to be addressed so that all legitimate emailers can be confident that their brand reputations do not suffer further consequences from a flawed email infrastructure.

The third goal should be to discuss authentication implementation in the context of compliance with the CAN SPAM Act. Issues requiring greater clarity include those surrounding "forwarding" services and the definition of "sender" which is critical in order to determine the appropriate entities to authenticate. Many refer-a-friend services and multiple advertiser promotions today are on hold until CAN SPAM Act compliance questions are answered. As a provider of such services, Experian/CheetahMail is unclear which party needs to be authenticated in the process and exactly how to authenticate an individual initiator who utilizes our forwarding service. Depending on the answers to these questions, the future of these basic email services is in question.

A final goal is to outline a timeline and path for multi-tiered authentication approaches across the Internet. The issues discussed in this response outline only the first phase of authentication. Another phase being discussed is that of cryptography, where each message sent is "signed" and authenticated by the receiver, rather than solely verifying the domain. While cryptography could be a complimentary solution to domain authentication, a discussion of how it could be implemented without intellectual property or costly resource ramifications should be enumerated. In addition, there have been increasing discussions of adding both accreditation and reputation services that track the success of a senders messaging efforts with authentication systems. While we believe accreditation and reputation is important, we are also concerned that such services may have a negative impact on the success of email due to faulty reporting systems. These services could also be considered collusionary if they are profiting from a monopolistic relationship with receivers governing the actions of legitimate business recipients. These issues could certainly be addressed, and the FTC's insight into their potential success could be very helpful.

***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.***

There are two key next steps following domain-level authentication. The first is to consider message-level authentication such as those through various cryptography proposals. These proposals need to ensure ease of use, open access, and limited costs for implementers. The second step is a careful review of the domain registration process, and the promulgation of "authenticated" spammers and phishers. Only after a series of consumer and business verification checks as well as confirmation of non-infringement of existing trademarks should a domain be registered to a party. If this system is not reviewed by the Commission and/or ICANN, then we will continue to see large volumes of spam and phishing and authentication will only solve a portion of the problem.