Comment #: 35

GoodmailSystems™
restoring trust in email™

September 30, 2004

Federal Trade Commission
Office of the Secretary
Room 159-H (Annex V)
600 Pennsylvania Avenue,NW
Washington, DC 20580

Subject: Email Authentication Summit
Comments (Matter Number P044411)

Dear Sir or Madam:

The following represents Goodmail Systems' response to select questions identified for discussion at the upcoming Email Authentication Summit.

We believe we will find this input very valuable.

Sincerely,

Maxine Graham
VP, Marketing
Goodmail Systems
650 230 7737
maxine@goodmailsystems.com

Email Authentication Summit

Comments (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.

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.

The following answers both questions #1 and #30 above.

The industry consensus is that an authentication standard alone would not result in a significant decrease in spam. Such a standard would reduce – but not eliminate – the spoofing of domains. To fight spam successfully, receiving ISPs must take additional measures beyond authentication, such as verifying reputation and changing the economics of email.

Fundamentally, what authentication does is enable a receiving ISP to determine whether a message comes from its purported sender. Even if the authentication standard succeeds in this regard, this information is not enough to determine that the sender is well-behaved. Indeed, sources have reported that spammers are already adopters of the SPF standard and publish their SPF records; relying upon SPF authentication alone would currently enable the successful delivery of spam – the very thing SPF aims to protect against! Ultimately, ISPs have no choice but to use a reputation database. By the same token, a reputation database that does not use some form of authentication would be completely crippled as any sender could claim another's reputation. Thus, both authentication and reputation are key components of a final solution.

What form should this authentication take? Herein lie several options of identity authentication. As we know, Sender ID and Domain Keys provide proof that a message was delivered (Sender ID) or originated (Domain Keys) from the owner of a given domain. Alternatively, a comparable authentication mechanism that verifies the "human"/"offline" identity and that provides a secure token of this identity inside the email message may serve equally well. (Such an authentication mechanism is part of Goodmail Systems' platform in which a sender would not be able to purchase stamps without verification of their identity and ownership of their domains.) In constructing the solution, any reputation database operator needs to perform this identity authentication while also screening against misleading domains that appear to be phishing domains. This makes it even tougher for scam artists to spoof a trusted domain and increases the solution's value as anti-phishing tool.

Next, in fairness to legitimate senders, the reputation database operator must have the means to monitor senders' behavior and the means to score their reputation fairly, transparently, and reliably. To achieve this, message recipients must have a means to report complaints either to their ISP or to the third-party reputation database operator. Next, the complaint system must have a mechanism for verifying that a complaint is valid, a prerequisite of which is that the recipient really did receive a message from that particular sender. Finally, a reputation database operator must also be able to capture the total number of messages sent from each sender (the denominator in the complaint rate calculation).

Because we might not expect every sender to have a record in the reputation database, recipients must be able to differentiate between the good messages and spam to make decisions of which messages to read and trust and which to ignore. For this, an ISP must implement some form of visual differentiation – an inbox marker or label – as trustworthy, non-spoofable proof that a message's sender is reputable. Examples of creative phishing attacks have shown us that spammers will go to great lengths to display a misleading address, with the result that recipients can no longer simply scrutinize a URL to determine if it is trustworthy. Instead, recipients need a visual label that confirms that a message is good so they can better discriminate against those suspicious bank account emails and other phishing attacks. Note that, in a world where recipients believe their messages are being screened and/or authenticated, having no label on good messages may leave the recipient to assume that all messages are good and possibly set false expectations; inbox labeling helps diffuse this risk as well.

With these measures of authentication, reputation database, and inbox labeling, recipients are still vulnerable: spammers will try their hardest to find ways to game reputation systems. For example, a reputation database could be exploited by malicious senders who establish a positive reputation by first sending benign messages and then suddenly use that reputation to send spam. Not only will a reputation database operator require a good screening process to detect suspicious senders before they participate, this alone would not stop spammers from trying to game the reputation system. Ultimately, the only measure that can truly stop spammers is changing the economics of spam: require senders to pay money commensurate with the volume of messages they are sending. This is the truest way to discourage spammers and also has the benefit of encouraging senders to use good sending practices. Note that Goodmail Systems believes that consumers should never have to pay – only those who economically benefit most from sending the messages, namely commercial volume senders, should pay.

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.

Although an authentication standard itself might or might not directly cause messages to be labeled as false positives or false negatives (we will defer to other technology experts to answer this point of view), the real issue is that authentication is not a complete solution to the spam problem (as discussed elsewhere in this document) and ISPs will have to continue to filter messages, a process known to generate many false positives and false negatives. The only way to eliminate false positives would be to provide a solution complete enough that ISPs felt comfortable giving preferential treatment to the reputable messages and delivering them straight to the inbox, bypassing the spam filters for those messages. Moreover, in a world where people think authentication works, consumers may have misplaced higher expectations of these self-authenticated senders, especially if the messages do not carry a label to distinguish them as being authenticated.

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

As long as the authentication standard were domain-based, not IP based, then there should be no problem to outsourced email services providers because they would create a domain for each client. Note that a good reputation system must track the reputation across all parties involved in the message (i.e., both the sender and the mailer).

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).

Sender ID and Domain Keys will have moderate costs borne by the ISPs. However, the significant cost is in managing the reputation system, which is much more complex than authentication. The cost of the reputation system may be assumed by either ISPs or senders or both, and ultimately this decision rests with the reputation database operator and their customers. If assumed by ISPs, then the cost would likely be passed onto consumers. It is Goodmail Systems' opinion that the best solution for all is that commercial volume senders pay to guarantee the delivery of their messages so that ISPs and consumers do not pick up this tab.

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.

Yes, transmission times could be adversely affected with senders having to make an external query to determine reputation status. For this reason and many others, Goodmail Systems believes a token-based system is superior. In Goodmail Systems' model, a secure token is inserted into the headers of an email message; when the message is received at an ISP, the token is verified locally and asynchronously, allowing for the efficient and speedy delivery of the message while not incurring real-time transactions to a reputation source.

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

An authentication system alone is unlikely to prevent phishing. Although some forms of spoofing would be eliminated, other forms would continue – such as creative ways to use so called "cousin" domains that appear similar to ones consumers are already familiar with (e.g., such as by adding the suffix "custserve.com" after the primary domain, such as help@YourBank.com would become help@YourBank.custserve.com).

However, with a smart reputation database, consumer understanding and inbox labeling, this problem could be solved. Recipients would learn that all messages coming from their bank had a specific label on the message indicating a trusted, verified source. Anytime the recipient received a future message without the label, they could choose to ignore the message and avoid any hyperlinks contained in the message.

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

Spam is a complex, ever-changing, organic problem and the solution will be similarly complex, evolutionary, and organic. The winning solution against spam will not be a single initiative but many. It will not be driven solely by technology, new legislation, authentication approaches, reputation systems, or any other singular dimension. All will come into play. The various stakeholders feel the pain of spam in different ways and will view solutions accordingly. In that regard, the FTC and all current stakeholders must also evaluate another significant factor in this equation – the economics of the problem – and the increasing financial burden borne by one key set of stakeholders – the ISPs – in fighting spam.

The more engagement on the subject by the various stakeholders the more likely progress will be made. The FTC and the summit can be catalytic forces to drive new thinking, careful consideration, discussion, and action. The FTC and the Summit can also serve to emphasize the significance of the problem and the need for the collective stakeholders to take diligent and constructive action. The Internet has become a significant engine of commerce and economic growth. But the ill-health of email has reduced consumer perception of the medium's purpose and reliability, putting that commerce engine, and in fact the whole e-commerce economy, at risk. Consumer trust in email must be restored and the FTC can help effect that result.