Comment #: 13

ESPC
Email Service Provider Coalition

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

SENT VIA EMAIL to authenticationsummit@ftc.gov

RE: Email Authentication Summit – Comments
Matter Number PO44411

Dear Secretary:

On behalf of the Email Service Provider Coalition, I am happy to provide the following responses to the questions posed by the FTC in advance of the Email Authentication Summit. The ESPC will separately submit a request to participate in the Summit.

Questions:

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.

There are a number of factors that have created the environment in which spam can thrive. But one of the most critical elements is the fact that email is "spoofable" – meaning that spammers can misrepresent, or obscure, their identity as messages are sent. By hiding their identity, spammers are able to avoid accountability for their practices. As a result, the *impunity of anonymity* has severely hampered our efforts to respond to spam.

Unfortunately, anonymity is part of the fundamental architecture of email. The Simple Mail Transfer Protocol (SMTP) was never designed to include authenticated identity of the sender of a message. In many ways, SMTP allows spoofing and misrepresenting of identity within email messages. Broad changes to SMTP are difficult and time-consuming. As a result, there has been a significant focus on developing authentication tools that can be added without changes to the fundamental architecture of email delivery.

The major authentication proposals (Sender ID, SPF, and Domain Keys) are all mechanisms for identifying various parties involved in sending a message, such that

identity based spam reduction techniques could be developed. Each one of these authentication proposals performs a different function and, as a result, has different merits.

Arguably, authentication will not be embraced by spammers. A spammer that elects to authenticate email messages will be providing a more reliable mechanism to defeat the anonymity of SMTP. In other words, they will be opening themselves to accountability for their practices. But again, it is unlikely that spammers will adopt authentication schemes.

If spammers will not authenticate their messages, one could easily ask: "How can this reduce the amount of spam?" It is indeed true that authentication, standing alone, will probably not reduce spam. (This is particularly true with the more advanced authentication schemes, such as Sender ID and Domain Keys.) It will however, have a direct effect on phishing (see question 15). More importantly, authentication will allow legitimate sender to have their messages recognized as legitimate and routed directly to inboxes. This allows ISPs to respond to the concerns associated with false positives – legitimate emails that are blocked inappropriately by anti-spam measures employed by the ISP.

If an ISP can distinguish between legitimate (authenticated) messages and unauthenticated messages, they will be more likely to aggressively filter and restrict the delivery of spam into their subscribers' inboxes. ISPs are currently hesitant to "turn up the dials" on their anti-spam efforts due to the corresponding rise in false positives. By authenticating legitimate messages, ISPs can be more confident as they increase the intensity of their anti-spam efforts.

It is in this way that authentication can have an indirect effect on the amount of spam received by consumers. Authentication will directly reduce the amount of phishing in the marketplace today. It will also allow ISPs to be more aggressive in their anti-spam efforts as concerns associated with false positives are abated.

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 proposed authentication schemes layer on top of the Internet protocols, and thus are compatible with the existing infrastructure. SenderID proposes an optional new parameter in SMTP which creates some efficiency for those who choose to implement it.

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.

All of the proposed authentication mechanisms require additional software for receivers. The software for receiver performs the authentication algorithm. The

algorithms are not complicated and have been implemented in scripting languages.

All of the proposed authentication mechanisms require that senders publish additional information in DNS. Allowing small senders to do so in a manner that is comprehensible to a small business owner will require the development of appropriate tools. These tools are not technically complicated but do require careful thought with respect to messaging and instructions for the user. We expect that they will improve over time.

Domain Keys requires that senders sign portions of the message. This will require additional software and in some cases additional hardware for senders.

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

Deployment of any new Internet protocol or standard takes several years. We recommend that receivers initially simply label unauthenticated messages as such, and continue to apply their existing filters until all legitimate senders have had reasonable opportunity to accurately publish their records. A reasonable opportunity includes access to tools. We suggest that one to two years should be sufficient.

As discussed above, we expect that ISPs will increase the intensity of application of anti-spam efforts as more legitimate email is authenticated.

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.

Both SPF and SenderID allow senders to publish partial records. This facilitates deployment by allowing a sender to incrementally publish authentication information for their mail. This feature is important for senders of all sizes – currently there is no need to coordinate between the various aspects of mail within an organization or the tools it uses. Large senders generally do not have a centralized list of their mail servers. Small senders may use different providers for personal, transaction, and marketing email messages.

A partial record will generate an authentication result of "pass", "fail", or "don't know". The "pass" and "fail" cases, assuming the sender has published a correct record, will be accurate. The "don't know" case is the same as having no record; in some senses this feature exists to prevent senders from having to declare all of their mail servers or none of them.

A false "pass" can result if either the DNS records or TCP/IP (network) connection is high jacked. These are both technically extremely difficult spoofs to execute, and both will be readily apparent to the domain being spoofed.

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?

None of the authentication standards are mutually exclusive but they are not interoperable. Senders will need to implement all of them in order to reliably have their mail pass authentication checks. In other words, if Mail Server A wants its mail to be accepted by Mail Server B, then Mail Server A must implement standard Y as well as standard X.

Where the standards perform essentially the same task a proliferation of standards imposes costs on senders and, via the proliferation of DNS records, in the Internet itself.

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

For a standard to be useful it must be freely available to all senders and receivers, with no cost associated with rights to use the standard. Otherwise it becomes increasingly costly for senders to implement all of the standards. Cost based standards will encourage competition from a variety of free or lower cost standards, resulting in standards proliferation and the costs associated with the proliferation itself.

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

Both SPF and SenderID validate the "last hop"; that is, the last server that touched the message. Consequently, both require that the forwarder both perform authentication on the message before forwarding, and mark the message as forwarded. Marking the message as forwarded has been considered a best current practice for many years.

Message signature solutions such as Domain Keys provide end-to-end authentication.

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).

Authentication essentially requires that either the sending server mark the message that they are sending on behalf of another domain, or that the author of the message explicitly authorize the server's domain to send on their behalf. For example, if Company A uses mobile service X, and trusts mobile service X to properly check passwords and otherwise implement suitable security policies, then Company A

might simply authorize mobile service X to act as a Company A server. If Company A is not that organized, or has legal or other problems with delegation at that level, mobile service X can take responsibility for the message themselves, treating it much the way forwarded mail is treated.

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

Mailing lists are essentially forwarders; the user sends a message to the list manager, which then forwards it to all of the list members. Please see the discussions on forwarding.

All of the proposed authentication standards require that the client, via records in the DNS, explicitly authorize outsourced email services. This allows recipients to verify that the mail is indeed authorized by the sending domain. This is reasonable and necessary requirement on outsourced providers - otherwise the recipient has no way of knowing whether the third party was authorized or is simply forging.

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)

This depends on the definition of the responsible party. In any reasonable system, the "from" that is shown to the user is authenticated, and this requires that the sender or the sender's domain explicitly authorize the (in this example) the ISP SMTP network. Sender ID addresses this with the "responsible address" and "on behalf of" semantics. Domain Keys uses public/private key encryption to disseminate authority to send.

In the anti-spam mailing lists it has been pointed out many times that in order to stop forgery we have to stop doing things that are technically indistinguishable from forgery. This impacts all forms of mailing other than sending directly from the author's domain to the recipient's domain. The domain based authentication schemes (SPF, SenderID) give senders a choice of two ways to address this problem:

(a) Explicitly authorize other domains to send on their behalf. This is most appropriate for outsourced mail providers and third party mailing infrastructures with which the sender has a formal contractual arrangement.

(b) Have the sending infrastructure take responsibility for the message, showing to the user that they are sending on behalf of the author. This is most appropriate for mailing lists, forwarders, and other arrangements where the change of

infrastructure is controlled by the recipient rather than the sender - the recipient presumably only accepts this kind of mail from places he or she trusts. It also applies to some kinds of sender initiated infrastructure changes.

There are a number of less obvious cases, for example sending mail from a hotel Many corporations simply won't permit sending through the infrastructure of a random hotel with their domain name in any way associated, and will require their members to connect to the VPN or other corporate infrastructure to send corporate mail. For chatty personal mail however, approach (b) above will usually be more than sufficient.

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

WebMail is just another kind of mail client. It may be very secure or not secure at all, depending on the practices of the mail provider.

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.

Domain Keys is a cryptographic solution and it does impose a per message computation cost on both the sender and the receiver. However this cost is linear with volume and thus does not create a scaling problem.

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).

Domain Based Authentication (SPF, SenderID):

There will be costs for participants in the system except consumers. For senders, there is a one time cost of finding all of the ways the domain sends mail - for large, decentralized corporations this may represent significant effort. For small senders this is very straight forward. All senders must maintain additional records in the DNS, which, given the current structure of these proposals, represents a cost but a very small one.

Recipients bear most of the costs, in that they have to perform the authentication validation. They also get most of the benefit, in that authentication allows recipient systems to more accurately and quickly discard forgeries, as well as enabling more accreditation and reputation systems to identify spam.

Cryptographic Solutions (Domain Keys):

Cryptographic solutions but a larger burden on senders, in that they must cryptographically sign various portions of the message. Signing is more expensive than verifying a signature, but both are more computationally intensive than the IP address matching used by the domain based authentication schemes.

Cryptographic solutions put no burden on the consumer.

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.

ISPs that do not participate in the authentication scheme of the recipient domains will presumably see their mail subject to stricter filtering, tagged as unauthenticated, dropped on the floor. It is reasonable to suppose that different domains will have different policies, but differential treatment is at some level the whole point. Early in the deployment phase, where many senders will not yet have published complete records, the differential will presumably be mild - either tagging or additional filtering. As adoption spreads receiving domains will be able to apply stricter and stricter controls without significant risk of false positives. This will create a dynamic that accelerates adoption as both senders and receivers recognize and see the benefits of authentication.

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.

Any Internet-wide authentication system must support incremental adoption on a domain-by-domain basis. SPF, Sender ID, and Domain Keys all support a distributed and incremental adoption. It is reasonable to suppose that broad adoption by the major domains will take a year, and complete adoption five to ten years.

It is important to note that authenticated email solutions may be adopted quickly by ESPs. Indeed, the members of the ESPC are largely in compliance with SPF at this point, and Sender ID support is expected within the next few months.

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.

Please see the discussions of cost above. The impact on transmission times would be negligible for SPF, Sender ID, and Domain Keys. For hashing and proof of works schemes the transmission delays could be significant.

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

All domain based authentication schemes assign responsibility to the domain, which may choose to protect the anonymity of senders. The domain becomes a tag that is used to group all mail from an organization; absent an accreditation system there is nothing that ties a domain to a real world person or entity.

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

Schemes that affirmatively validate the domain that the user sees will greatly reduce phishing. Domain Keys and Sender ID (but not SPF) authenticate the user-visible fields. This will prevent the form of phishing where the sender impersonates 'bigbank.com', where 'bigbank.com' is the domain name of Big Bank. It will not prevent the form of phishing that is based on other domain frauds (exploiting assumptions), for example sending mail from 'bankbig.com', where 'bankbig.com' is not the domain name of Big Bank but is owned by an identity thief. Accreditation built on top of authentication will address other domain frauds directed at consumers.

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.

It is difficult to imagine that any organization managing domain names would be unable to publish the necessary authentication records. ISPs manage domain names. Many, if not most, small businesses do not manage their own domain and will need services from their ISP in order to implement authentication. The tools that exist today for updating DNS records are targeted at ISPs and domain administrators.

For any authentication standard to have broad adoption it must integrate easily into the existing infrastructure, with minimal costs to both recipients and senders. Domain based IP address authentication (SenderID, SPF) is very compatible with existing software and infrastructures - mail servers already do large numbers of DNS lookups in order to send and deliver mail.

The members of the ESPC are eager to promote the rapid adoption of consistent, ubiquitous tools for email authentication. We look forward to the email authentication summit.

Sincerely,

J. Trevor Hughes

Executive Director

Email Service Provider Coalition

266 York Street, York, ME 03909 Phone: 207-351-1500 Fax: 207-351-1501 www.espcoalition.org