



August 30, 2017

Federal Trade Commission  
Office of the Secretary  
600 Pennsylvania Ave NW  
Suite CC-5610 (Annex B)  
Washington, DC 20580

Filed Electronically <https://ftcpublic.commentworks.com/ftc/canspamrulereview>

Re: CAN-SPAM Rule, 16 CFR part 316, Project No. R711010

Dear Secretary Clark:

Thank you for providing an opportunity to comment publicly on the CAN-SPAM Rule.

The CAN-SPAM Act has been enormously effective in cleaning up the email ecosystem over the past decade and a half, reducing costs for both businesses and consumers by limiting the amount of unsolicited commercial email that we all must deal with.

Email has grown even more ubiquitous in the years since the CAN-SPAM Act was first passed in 2003. Now, 98.4 percent of consumers check email daily [1], and the average white-collar worker spends 30 hours a week checking email [2].

While spam filters and other algorithms have prevented a large amount of spam from reaching users' inboxes, the volume of spam remains extremely high. Cisco estimates that 60 percent of all email is spam or malware [3].

CAN-SPAM has not solved the spam or email malware problem, but it has provided a valuable enforcement tool for deterring the worst offenders.

With a few judicious adjustments to the FTC's CAN-SPAM Rule, this law can become even more effective at making email more trustworthy and reliable, and at a very small or zero cost to businesses.

**ValiMail, Inc.**, 180 Montgomery St., 18th Floor, San Francisco, CA 94104

**In regards to question 6 (“What modifications, if any, should be made to the Rule to reduce any costs imposed on consumers?”):**

The text from the Act refers to:

a “from” line (the line identifying or purporting to identify a person initiating the message)

In practice, senders now use multiple headers (“lines” per the Act) that purport to identify the person or organization who initiated the message, such as the Return-Path and DKIM-Signature headers. But these headers are not usually presented to the user in a mail client.

The FTC should add a definition to clarify that the “from” line referred to in the CAN-SPAM Act should be interpreted to refer only to the From field that is visible to the end user (in technical terms, this is the RFC5322.From field), not the Reply-to, DKIM-Signature, or Return-Path fields.

We join with the Online Trust Alliance in recommending that the definition of ‘From’ in the Rule be specified as the ‘From’ that is presented to the user in their email client [4].

Doing so would clear the path for the FTC to enforce CAN-SPAM violations that involve impersonators who put fake addresses in the From header, the most common technique used in phishing attacks that try to trick recipients into downloading malware or giving over their account credentials [5].

With enforceable consistency in the use of the From field, it would be much easier for consumers to accurately identify who is sending them email, saving them time and increasing their ability to avoid spam and malware.

**In response to question 12 (“What modifications, if any, should be made to the Rule to account for changes in relevant technology or economic conditions? What evidence supports the proposed modifications?”):**

When the CAN-SPAM Act first passed, spam was a pernicious problem that the Internet community had only started to get a handle on.

A lot has changed since then. For instance, content filters have become immensely more sophisticated and effective, while receiving servers have learned to use sender reputations to quarantine the worst offenders while greenlighting the good actors.

Since the Act passed in 2003, we've also seen the introduction of email authentication standards aimed at stemming the tide of spam and phish by making senders more accountable for the emails they transmit: Sender Policy Framework (SPF) has been in development since 2003 and in wide use since 2006; DomainKeys Identified Mail (DKIM) since 2004; and Domain-based Message Authentication, Reporting, and Conformance (DMARC) since 2012.

With these standards in place, it's now possible for senders to identify themselves positively and reliably. Specifically, email authentication with DMARC ensures that the From header visible to users in their mail clients matches the headers authenticated by SPF and DKIM, and allows domain owners to specify policies that prevent delivery of non-authenticating messages.

With DMARC set to enforcement (a policy of p=quarantine or p=reject), domain owners sending email get all the value that the CAN-SPAM Act provides with respect to positive identification of the sender — one of the core requirements of the Act.

If you authenticate your email, then email that says it's from you really is from you. This is an extremely valuable addition, and adds technological teeth to the policies that the Act lays out. The FTC should strongly recommend email authentication with a policy of enforcement.

This also has a compliance benefit. Businesses and other organizations that implement DMARC with an enforcement policy (p=quarantine or p=reject) can protect themselves against CAN-SPAM violations by ensuring that their domains are not misused by unauthorized third parties.

Email authentication also opens up some interesting possibilities for battling spam. Given the widespread use of authentication among email receivers, these standards are now effective tools for ensuring compliance with the CAN-SPAM Act's requirement that businesses not use false or misleading header information.

Additionally, the presence or absence of email authentication is increasingly becoming a valuable tool for spam filters to use in evaluating inbound email.

What's more, this aligns with the FTC's own point of view, as it recommended the use of DMARC in March, 2017 [6]. The FTC should extend that recommendation through its CAN-SPAM Rule and other communications around spam and commercial email.

Additionally, we recommend that the FTC add a section on email authentication to its CAN-SPAM compliance guidelines for businesses [7].

CAN-SPAM is not perfect but it provides a valuable enforcement tool that has helped contain the growth of spam. With a few modifications to the FTC's Rule, CAN-SPAM could remain effective against spam and even become more useful to control spam and email-borne malware.

Respectfully,

Peter Goldstein  
CTO and Co-founder, ValiMail

Seth Blank  
Director of Industry Initiatives, ValiMail

Next page: Sources

[1] BlueHornet research:

<http://www.businessinsider.com/how-often-do-people-check-their-email-2015-8>

[2] Adobe research: <https://blogs.adobe.com/conversations/2015/08/email.html>

[3] Cisco: <http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017>

[4] Online Trust Alliance recommendations:

<https://otalliance.org/news-events/press-releases/online-trust-alliance-responds-ftc-fee-dback-request-suggested-can-spam>

[5] GreatHorn research: <http://info.greathorn.com/cloud-email-security-challenge>

[6] FTC recommendations on DMARC:

<https://www.ftc.gov/news-events/blogs/business-blog/2017/03/want-stop-phishers-us-e-email-authentication>

[7] FTC guidelines on CAN-SPAM compliance:

<https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business>