ESPC
Email Sender & Provider Coalition

August 29, 2017

Via Electronic Submission to https://ftcpublic.commentworks.com/ftc/canspamrulereview

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex B)
Washington, DC 20024

RE: CAN-SPAM Rule, 16 CFR Part 316, Project No. R711010

To Whom It May Concern:

The Email Sender and Provider Coalition ("ESPC") hereby submits its comments in response to the Federal Trade Commission's request for public comment on its review of the CAN-SPAM Rule, 16 C.F.R. Part 316 (the "Rule").[1] The ESPC appreciates this opportunity to comment on how the FTC can continue to improve the health of the email ecosystem through the reduction of unlawful spam.

The ESPC is a cooperative group of industry leaders working to create solutions to the continued proliferation of spam and the emerging problem of legitimate email deliverability. ESPC's membership provides mail delivery services to an estimated 250,000 clients, representing the full breadth of the U.S. marketplace. The ESPC's mission is to advocate on behalf of email senders, providers, and other digital marketers operating globally in the online, mobile, and social media environments in favor of global laws and self-regulatory efforts that balance consumer protection and business innovation; to educate its membership on current and emerging business and legal developments affecting its membership; and to continue to develop and refine best practices that foster innovation, industry growth, and consumer trust.

New and existing ESPC Members must adhere to a Pledge that forbids spam by requiring informed consent before sending commercial email. The Pledge also prohibits the surreptitious collection of email addresses, including through either harvesting or scraping, and requires the use of authentication methods when sending commercial email messages, like SPF and DKIM.

[1] 82 Fed. Reg. 29254-29256

Below, the ESPC responds to several of the specific questions posed by the FTC in its call for comments on the CAN-SPAM Rule.

A. General Issues

FTC Question 7: What benefits, if any, has the Rule provided to businesses, including small businesses? What evidence supports the asserted benefits?

The ESPC believes that the Rule has resulted in three principle benefits to businesses, including small businesses: (1) the creation of a national standard for commercial email; (2) the provision of a reasonable grace period for implementing opt-outs; and (3) a strong history of enforcement by the FTC and state attorneys general that has protected consumers and helped to foster a healthy marketplace for legitimate email senders.

First, the CAN-SPAM Act and Rule has helped create a single, nation-wide standard for commercial email in the United States. The CAN-SPAM Act itself contains a strong preemption provision: "This chapter supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto." 15 U.S.C. § 7707(b)(1). This strong statutory preemption language has been supplemented by the FTC's CAN-SPAM Rule, which provides a rubric for identifying the types of email that are regulated as "commercial electronic marketing messages" ("commercial emails"), as that term is defined by the CAN SPAM Act, 15 U.S.C. § 7702(2), and prohibits the charging of fees to consumers to opt-out of such messages. The absence of multiple, divergent state and local standards governing electronic messages allows businesses to develop compliant solutions at a national level and avoid the costs of designing custom approaches to account for local variances.

Second, the CAN-SPAM Act has established a ten-day grace period for processing opt-outs. This grace period is especially beneficial to smaller businesses who often must process opt-outs in a semi-manual fashion and without the assistance of a fully automated solution to do so because they cannot afford the cost of such a solution. For larger businesses, the grace period provides time to synchronize systems across a company and the company's vendors. Although this process is generally automated, the process of exchanging and matching information can take time. The statutory ten-day period, which was not revised by the FTC in the current Rule, allows businesses the time needed to comply with an opt-out request while also directing businesses to respond to consumer requests with reasonable speed.

Third, the FTC and state attorneys general have used their authority under the CAN-SPAM Act and Rule to punish bad actors engaged in deceptive or unfair SPAM practices. These enforcement actions have both protected consumers and helped to foster a healthy marketplace for legitimate commercial email senders, helping to ensure that consumers receive appropriate and lawfully sent commercial emails. Notable recent enforcement actions include *FTC v. Croft* (S.D. Fla., 9:17-cv-80425), in which the FTC enjoined a spammer who purported to be authorized by the FTC to remove spyware from recipients' computers, and *FTC v. Tachht, Inc.*,

P.O. Box 478, Kennebunk, ME 04043 | 207.351.5770

(M.D. Fla, 8:16-cv-1397), in which the defendants allegedly used spam emails to direct consumers to fake news websites about the defendants' weight-loss products. In addition to these recent actions, the FTC has a long track record of curtailing unlawful emailing practices and imposing significant civil penalties. *See, e.g., FTC v. Sale Slash, LLC* (C.D.Cal. 2:15-cv-03107) (another FTC enforcement action involving weight-loss products and fake news sites, which resulted in a substantial judgment and asset seizures); *FTC v. Atkinson* (N.D. Ill. 08-cv-5666) ($870,000 payment with the remainder of $1.1 million judgment suspended); *FTC v. Sili Neutraceuticals* (N.D.Ill. 1:07-cv-04541) (resulting in default judgment of over $2.5 million); *FTC v. Valueclick* (C.D.Cal. 08-cv-01711) (resulting in penalty of $2.9 million).

FTC Question 11: What evidence is available concerning the degree of industry compliance with the Rule?

ESPC members comply with the Pledge, which requires opt-in consent to receipt of all commercial email, a higher standard than the one imposed by the CAN-SPAM Act and Rule. The Pledge states, in relevant part: "Commercial email (email messages, the primary purpose of which is the commercial advertisement or promotion of a product or service) must not be sent to an individual's email address unless the prior, affirmative consent of the individual has been obtained." The Pledge also requires prompt processing of opt-out requests, prohibits deceptive subject and message content, requires compliance with laws related to commercial email, and bars "surreptitious methods" (e.g., scraping or harvesting) of email address collection. Adoption of the Pledge demonstrates a voluntary commitment to a higher standard than now exists under current law in the United States.

FTC Question 13: Does the Rule overlap or conflict with other federal, state, or local laws or regulations? If so, how?

The ESPC does not believe the Rule conflicts with any other federal, state, or local laws. In general, inconsistent state and local laws would be preempted by 15 U.S.C. § 7707(b)(1). Although CAN-SPAM does not preempt generally-applicable state laws, including those which generally prohibit fraud or unfair and deceptive trade practices, the ESPC does not believe that such laws create significant conflicts with CAN-SPAM. State laws prohibiting fraud and protecting consumers from unfair or deceptive trade practices are consistent with the requirements of CAN-SPAM and the FTC's Section 5 enforcement authority. *See* 15 U.S.C. § 7707(b)(2).

B. Specific Issues

FTC Question 2. As discussed above, the Rule tracks the CAN-SPAM Act in prohibiting the sending of commercial email to a recipient more than ten business days after the recipient opts out. Should the Commission modify the Rule to reduce the time-period for processing opt-out requests to less than ten business days?

The ESPC strongly believes that the period provided for processing an opt-out request should not be shortened. As noted above in response to Question 7, small businesses that may not be able to afford automated opt-out solutions often require ten days to process an opt-out

P.O. Box 478, Kennebunk, ME 04043 | 207.351.5770

request manually. In addition, it may take ten days for a large company to implement an opt-out across multiple databases or servers, especially if the company uses several vendors for sending email marketing communications. Synchronizing these various databases in a manner that avoids disruption of active operations requires the full 10-day statutory period. Providing ten days for the processing of opt-outs creates a realistic implementation period for small and large businesses, while still ensuring that the consumer's wishes are implemented in a timely manner.

FTC Question 3: Should the Commission modify the Rule to specify additional activities or practices that constitute aggravated violations?

The Commission should consider including the practice known as "snowshoeing" as an aggravated violation.

3(a). Why or why not?

Snowshoeing involves the use of multiple domains and IP addresses (obtained from different ISPs) to artificially dilute reputation metrics and avoid spam filters by ISPs (the "receivers" of email). This strategy keeps the volume of emails sent very low (in some cases, only a few hundred emails are sent per domain or IP address) while permitting large aggregate volumes to be distributed across hundreds or thousands of IP addresses and domains. Snowshoeing allows spam to be spread across multiple networks in an anonymous fashion, analogous to the prohibited practice of using an unsecured relay.

3(b). What evidence supports such a modification?

Senders engaged in snowshoeing present a real risk to consumers, and often send emails related to phishing, fraud, or identity theft schemes. Content-based filters have been proposed as a solution to snowshoe spam, but privacy concerns limit the effectiveness of such filters by placing restrictions on how email content can be reviewed and screened. As a result, current tools may not be adequate to protect consumers from snowshoeing.

3(c). How would this modification affect the costs the Rule imposes on businesses, including small business?

The impact should be minimal. Most email service providers follow industry best practices and do not engage in snowshoeing. Small businesses sending email messages from a dynamic IP address may need to purchase a dedicated IP address and use one consistent domain in all headers.

3(d). How would this modification affect the benefits to consumers?

Prohibiting snowshoeing would bar a method of sending near-anonymous spam email messages. Filters and reputation metrics are more effective against non-snowshoe spam, allowing email recipients (again, the ISPs) to exercise greater control over the commercial email they receive. Consumers would also be better protected from the phishing, fraud, and identity theft schemes contained in the message sent using snowshoe methods.

P.O. Box 478, Kennebunk, ME 04043 | 207.351.5770

***

The ESPC appreciates the opportunity to submit comments in this important proceeding. If you have any questions concerning these comments, or if we may otherwise be of assistance in connection with this matter, please do not hesitate to contact me at 202-663-6267.

Sincerely,

D. Reed Freeman, Jr.
Outside Counsel
Email Sender & Provider Coalition

WilmerHale
1875 Pennsylvania Avenue NW, Washington, DC 20006 USA
+1 202 663 6267 (t)
reed.freeman@wilmerhale.com

cc: ESPC Board of Directors

P.O. Box 478, Kennebunk, ME 04043 | 207.351.5770