

April 20, 2020

VIA EMAIL

The Honorable Mazie K. Hirono
United States Senate
713 Senate Hart Office Building
Washington, DC 20510

The Honorable Margaret Wood Hassan
United States Senate
324 Senate Hart Office Building
Washington, DC 20510

The Honorable Cory A. Booker
717 Senate Hart Office Building
United States Senate
Washington, DC 20510

Dear Senators Hirono, Hassan, and Booker:

Thank you for your April 13, 2020 letter (the "Letter") to Donuts Inc. ("Donuts") regarding the response of its registrar, Name.com, Inc. ("Name.com"), to online exploitation of the novel coronavirus ("COVID19"). Name.com takes all compliance and potential violations of its acceptable use policies seriously. While COVID19 presents an unprecedented public health and economic crisis, Name.com has a long history of taking action on registrations that exploit tragedies. COVID19 is no exception and Name.com has put its veteran abuse and fraud team on alert to ensure that any abuse related to COVID19 is dealt with quickly.

As explained below, Name.com takes a comprehensive and robust approach to reports of abusive domain registrations. Name.com is proud to work with federal and international law enforcement, state officials, and those in the domain industry to ensure Name.com's policies, procedures, and outreach provide an appropriate and effective response to abuse, especially COVID19-related abuse. Name.com is pleased to provide the following responses to the Letter's questions. For ease of reference, the questions in the Letter have been incorporated into this response.

1. What steps do you take to ensure that entities seeking to register domain names are legitimate, and not cybercriminals or other malevolent actors? Which, if any, of these steps have been added since the onset of the coronavirus pandemic?

Name.com exercises three primary efforts to promote legitimate domain name registrations. First, Name.com leverages both automated and human review of domain name registrations and activity on its platform. While COVID19 presents the world a novel and unique set of issues, for domains that exhibit COVID19-related abuse the methods are hardly unique, and thus Name.com's review processes are attune to combat them. Name.com's review process includes but is not limited to utilizing internal tools that flag domains potentially in violation of applicable policies and actively monitoring external feeds from a variety of organizations (e.g., Softlayer/IBM and Spamhaus) to identify trends of abuse. And, as you will hear from other registrars, while registrant intent or background is generally not reviewed prior to registration, Name.com is confident in the capability of its robust toolset and resources to guide its staff to act expeditiously and appropriately to identify and respond to reports of abusive registrations.

Second, Name.com's experienced fraud and abuse team act quickly to review and suspend, terminate and otherwise remediate domains that are involved in unlawful or harmful activity. This includes applying Name.com's stringent policies to each domain that receives a complaint for COVID19-related abuse, whether for phishing, installing malware or otherwise. Name.com's fraud and abuse team reviews each complaint with an eye toward timeliness and accuracy (e.g., typically within 24 hours). Each complaint is handled by a human being with specific experience with domain abuse and fraud, not automated response systems.

Lastly, Name.com leverages its longstanding partnerships with law enforcement to avoid exploitation of crises like the COVID19 epidemic. Since the onset of COVID19, Name.com has conferenced with the U.S. Federal Bureau of Investigations, the United Kingdom's National Crime Agency (the UK's lead agency on organized and cybercrime), the New York State Attorney General, industry partners, and trusted notifiers like LegitScript to monitor and take action against COVID19-related abuse. Additionally, Name.com is reviewing its registrations for COVID19 related terms and has included the new terms provided in the Letter in its fraud detection and mitigation programs. In addition to its existing abuse complaint contact (abuse@name.com), Name.com created a direct channel for law enforcement to use specifically for COVID19-related matters at covid19abuse@name.com. Name.com is pleased to make this new email resource available to your Senate offices for receipt of COVID19 related complaints.

2. What additional steps, if any, do you take to ensure that entities seeking to register domain names that contain coronavirus-related terms, such as "coronavirus," "covid," "pandemic," "virus," or "vaccine," are legitimate, and not cybercriminals or other malevolent actors?

As stated above, registrations including certain terms at Name.com are being reviewed as part of its COVID19 response. Accordingly, Name.com has added to its fraud and abuse detection list any terms suggested in the Letter that Name.com did not already include in its list. Domains reported and found to be violating Name.com's stringent policies and/or applicable laws will be reviewed quickly and, depending on the circumstances, either suspended or terminated.

3. What additional steps, if any, do you take to ensure that entities seeking to register domain names that reference drugs touted as potential treatments for the coronavirus, such as "remdesivir," "chloroquine," "hydroxychloroquine," "Plaquenil," "azithromycin," "metformin," "favipiravir," "interferon," "lopinavir," "ritonavir," or "arbitol," are legitimate, and not cybercriminals or other malevolent actors?

As part of its overall mitigation efforts targeting pharmaceutical-related abuse, Name.com has a longstanding "trusted notifier" relationship with LegitScript. While not required to do so, Name.com generally suspends or terminates registrations referred from LegitScript regarding pharmaceutical-related abuse. To further improve Name.com's response to these COVID19-related pharmaceuticals, and in response to your Letter, Name.com has added the terms in the Letter's question 3 to Name.com's reports. Domains reported and found to be violating Name.com's stringent policies and/or applicable laws will be reviewed quickly and, depending on the circumstances, either suspended or terminated.

4. What additional steps, if any, do you take to ensure that entities seeking to register domain names that reference Zoom, Google Classroom, Microsoft Teams, or other online communications platforms are legitimate, and not cybercriminals or other malevolent actors?

Name.com is monitoring the registration of terms related to the communication platforms like Google Classroom, Zoom, and Microsoft Teams. Domains impersonating these platforms fall squarely into Name.com's existing set of anti-abuse measures (i.e., anti-phishing) and will be suspended or terminated. As is detailed below, Name.com has not encountered significant amounts of abuse related to these platforms.

5. What steps do you take on an ongoing basis to ensure that registrants are not using their registered domains for unlawful or harmful activity?

Name.com's case volume has been low for COVID19-related complaints. Name.com's abuse and fraud team weighs all evidence provided by the complainant and even looks at the overall activity of the domain registrant on its platform. Domains in violation of Name.com's policies will undergo appropriate action, including suspension or termination of services. Name.com utilizes an internal tool that flags domains that may be used for nefarious purposes based on custom keyword entry even if no complaint about the domain is received.

As of April 15, 2020, Name.com has received less than 50 substantive complaints regarding COVID19, each of which has been reviewed and closed out. Most complaints stemmed from automated tools and approximately 5 came from law enforcement. Of these domains, 9 were suspended or terminated and the remainder were either not in active use (e.g., not connected to any content or showing auto-generated advertising) or were otherwise not violating Name.com's policies. This scenario is not atypical; many registered domains do not provide any content because they are held primarily for investment or speculative value. Preventing or blocking the registration of domains containing keywords that, as in the case of COVID19, have the potential to be used in abusive activities is problematic and has never been Name.com's practice. Name.com does, as noted above, take quick action in other ways after registration has taken place. Owing to its diligence and rapid response to unlawful or harmful activity, Name.com's reputation serves as a strong deterrent for abuse and other malicious activity on its platform.

6. What are the penalties for registrants found to be using their registered domains for unlawful or harmful activity?

Name.com's [Privacy Policy](#), [Acceptable Use Policy](#), and [Registration Agreement](#) provide sufficient and broad authority to take action on any illegal or malicious use of a domain, including abuse related to COVID19, testing, kits, pharmaceuticals, or anything related to the epidemic. For example, the fraud and abuse team routinely apply the following sections of the Name.com [Registration Agreement](#), to which all registrants of a domain name must agree prior to registering a domain, which provide ample latitude to take action against illegal use of COVID19 domains, including termination or suspension of a domain or any Name.com service altogether (emphasis added).

- **Section 4.B.ii: *You represent and warrant that [...] no Services are being procured for any unlawful or abusive purpose, including but not limited to the infringement of any intellectual property right or other right; the distribution of malware; the abusive operation of botnets; phishing, fraudulent or deceptive practices; [...] or any other activity in violation of any laws, rules, or regulations.***
- **Section 6A: *[W]e may reject, terminate or suspend the Services, including placing any domain name(s) on lock, hold, or similar status such as transferlock, at any time for cause, which without limitation includes [...] (ii) abuse of the Services; [...] (iv) allegations of illegal conduct or***

infringement of any third-party intellectual property right or other right, including violations of our Acceptable Use Policy; [...]. No fee refund will be made when there is a suspension or termination of Services for cause.

7. What steps do you take to cooperate with law enforcement when registrants are suspected of using their registered domains for unlawful activity?

As noted above, Name.com works closely with law enforcement at many levels, both domestically and internationally, to identify and take action on abusive domains. Domains in violation of Name.com’s policies will undergo appropriate action, including suspension or termination of the domain and any other service. With regard to COVID19 specifically, Name.com is already in contact with those professionals to ensure swift and effective disruption of domains attempting to exploit the epidemic. Name.com can provide contact information for those individuals upon request. Domains referred by law enforcement are reviewed by Name.com’s abuse and fraud team and mapped to the overall activity of the registrant on its platform. While all reports of abuse are handled quickly (see response 1 above), law enforcement inquiries are prioritized and receive responses that include greater background, specificity and information than others. Name.com is pleased to offer the same to your Senate offices if it should have any COVID19-related reports of abuse.

8. Since the start of 2020, how many applications have you received for domain names that contain coronavirus-related terms, such as “coronavirus,” “covid,” “pandemic,” “virus,” or “vaccine?” How many of these domain names have you registered? Please provide this information broken down on a monthly basis.

Since the start of 2020 and as of April 15, 2020, the following terms have been included in domains registered at Name.com, broken down by domains registered by month. Name.com has seen very few reports of abuse on domains containing these terms. It is worthy to remember that the number of domains registered typically does not correlate to active or malicious content. Many domains are held primarily for investment or speculative value.

	Jan. 2020	Feb. 2020	Mar. 2020	Apr. 2020	Total
coronavirus	14	38	270	30	352
covid	0	28	809	263	1100
pandemic	3	9	23	17	52
virus	32	59	455	74	620
vaccine	1	7	12	16	36

9. Since the start of 2020, how many registrations for domain names that contain coronavirus-related terms, such as “coronavirus,” “covid,” “pandemic,” “virus,” or “vaccine,” have you suspended, cancelled, terminated, or referred to law enforcement? Please provide this information broken down on a monthly basis.

As noted above, Name.com has seen very few reports of abuse on domains registered containing the terms highlighted in the Letter. In 2020, as of April 15, 2020, Name.com has suspended 9 domains with these terms, with 4 of those suspended in March and the remaining 5 in April.

10. Since the start of 2020, how many applications have you received for domain names that reference drugs touted as potential treatments for the coronavirus, such as “remdesivir,” “chloroquine,” “hydroxychloroquine,” “Plaquenil,” “azithromycin,” “metformin,” “favipiravir,” “interferon,” “lopinavir,” “ritonavir,” or “arbitol?” How many of these domain names have your registered? Please provide this information broken down on a monthly basis.

Since the start of 2020 and as of April 15, 2020, the following terms have been included in domains registered at Name.com, broken down by domains registered by month:

	Jan. 2020	Feb. 2020	Mar. 2020	Apr. 2020	Total
remdesivir	0	5	4	0	9
chloroquine	0	0	1	0	1
hydroxychloroquine	0	0	0	0	0
Plaquenil	0	0	0	0	0
azithromycin	0	0	0	0	0
metformin	0	0	0	0	0
favipiravir	0	0	0	0	0
interferon	0	0	0	0	0
lopinavir	0	0	0	0	0
ritonavir	0	0	0	0	0
arbitol	0	0	0	0	0

11. Since the start of 2020, how many registrations for domain names that reference drugs touted as potential treatments for the coronavirus, such as “remdesivir,” “chloroquine,” “hydroxychloroquine,” “Plaquenil,” “azithromycin,” “metformin,” “favipiravir,” “interferon,” “lopinavir,” “ritonavir,” or “arbitol,” have you suspended, cancelled, terminated, or referred to law enforcement? Please provide this information broken down on a monthly basis.

Name.com has received no complaints or references to abuse for domains containing the terms in question 11. Accordingly, Name.com has issued no related suspensions.

12. Since the start of 2020, how many applications have you received for domain names that reference Zoom, Google Classroom, Microsoft Teams, or other online communications platforms? How many of these domain names have you registered? Please provide this information broken down on a monthly basis.

Since the start of 2020 and as of April 15, 2020, only 2 domains (both in March) have been registered at Name.com containing terms related to the above listed online communications platforms.

13. Since the start of 2020, how many registrations for domain names that reference Zoom, Google Classroom, Microsoft Teams, or other online communications platforms have you suspended, cancelled, terminated, or referred to law enforcement? Please provide this information broken down on a monthly basis.

Both domains referenced in the response to question 12 of the Letter were reviewed, did not violate any of Name.com's policies, and did not otherwise present any malicious or unlawful activity. Accordingly, Name.com did not suspend or terminate either domain.

Name.com has an admirable history of disrupting cybercriminals and other malevolent actors on its platforms. As noted above, leveraging its comprehensive review systems, experienced abuse and fraud professionals, and relationships with law enforcement near and far provide Name.com a well-deserved reputation for vigilance. As the world faces an unprecedented threat in COVID19, Name.com will continue its unflinching reviews and take quick action on its platform to protect its customers, employees, and the Internet-using public.

Thank you again for sharing your concerns with Donuts and Name.com about fighting COVID19-related domain name abuse and the efforts you are making to protect Americans online during this unprecedented and challenging time. Should you have additional questions or concerns, please feel free to reach out to me personally. Given the closure of U.S. Senate offices during the COVID19 outbreak, this response is being sent to you via email only.

Yours sincerely,



Akram Atallah
akram@donuts.email
President and CEO
Donuts Inc. (parent of Name.com, Inc.)