NABP
National Association of Boards of Pharmacy

ROGUE RX ACTIVITY REPORT

Rogue Online Pharmacies in the Time of Pandemic: Capitalizing on Misinformation and Fear

No part of this publication may be reproduced in any manner without the written permission of the executive director/secretary of the National Association of Boards of Pharmacy.

©2020 by the National Association of Boards of Pharmacy. All rights reserved.

NABP

SUMMARY

Rogue internet pharmacy networks are run by criminal opportunists, and the coronavirus disease 2019 (COVID-19) pandemic has provided the perfect opportunity for illegal online drug sellers to prey on fearful consumers. These criminals are not new to the game; they are simply targeting a novel disease.

During the past several weeks, the National Association of Boards of Pharmacy® (NABP®) identified dozens of illegal online pharmacies that are actively peddling prescription-only drugs marketed as COVID-19 treatments. We also flagged hundreds of newly created domain names that do not yet appear active but, in the days and weeks to come, may be used to sell illegal coronavirus treatments. In our review, we found the following: (1) most active websites have clear ties to known criminal networks or their affiliates; (2) some newly created COVID-specific websites redirect users to established rogue network sites; (3) many domain names, both active and inactive, are clustered on "safe haven" registrars – a practice common among sophisticated internet pharmacy cybercriminals; and (4) the domain name registration information for almost all identified websites is anonymized, making it difficult for enforcement agencies to investigate these criminals.

In an effort to protect vulnerable consumers, government agencies are cracking down on COVID-related cybercrime. NABP applauds these efforts. Regulators, members of Congress, and state attorneys general are also asking the private sector for assistance. Many internet intermediaries have stepped up to the plate, shutting down fraudulent face mask, vaccine, and test kit sellers. However, illegal internet "pharmacies" continue, largely unabated, to peddle falsified, substandard, and dangerous drugs, including purported treatments for COVID-19. This behavior is predictable; these bad actors have been around for over 20 years. We can – and must – stop it now.

NABP calls on all internet companies to implement long-term policy changes that will have a significant impact on patient safety. Upon notification from authoritative sources, domain name registrars should immediately lock and suspend domain names that are used for illegitimate purposes. For domain names that are engaged in commerce, registries and registrars should provide open access to accurate, non-anonymous registration information. Search engines

should flag as dangerous, or deindex, known scam websites, as well as those websites that offer prescription drugs without requiring a prescription. By implementing these changes, internet intermediaries will protect patients during this scary and unprecedented time, and afterwards.

If significant action is not taken voluntarily by internet intermediaries, then NABP supports legislation that would require registrars to validate domain name registration information and make registration data accessible, as well as legislation that would require domain name registrars to immediately lock and suspend any domain name used to faciliate illegal activities that harm public health.

CRIMINAL INTERNET PHARMACY NETWORKS ARE CAPITALIZING ON THE PANDEMIC

NABP identified dozens of active websites that illegally offer prescription-only drugs for the treatment of COVID-19; we added these websites to our Not Recommended List.[1] The vast majority of these websites are run by well-known criminal networks, including Rx-Partners, EvaPharmacy, and Worldwide Drug Store.[2]

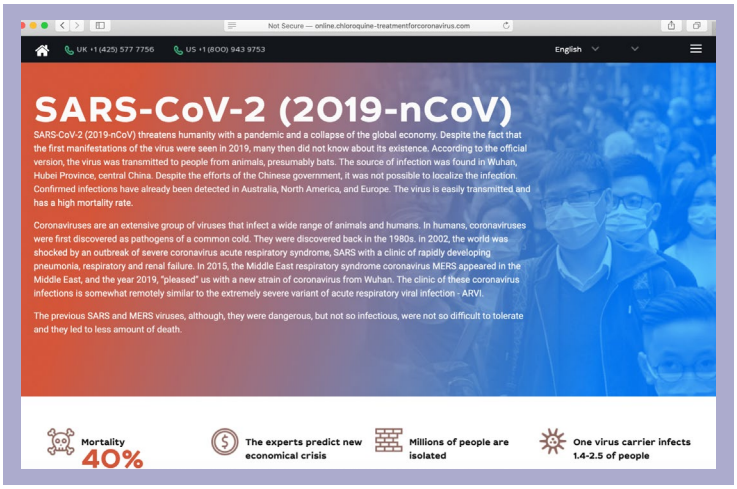
What are they selling? Currently, network affiliates are peddling a small selection of prescription-only drugs that have gained media attention as possible, but unproven, treatments for COVID-19. The most commonly offered drugs include chloroquine, hydroxychloroquine, azithromycin, and lopinavir/ritonavir. Chloroquine (Aralen®) and hydroxychloroquine (Plaquenil®) are antimalarial drugs that have received emergency use authorization from Food and Drug Administration (FDA) for the treatment of certain hospitalized COVID-19 patients.[3] Azithromycin is an antibiotic that is being used in combination with chloroquine and hydroxychloroquine. Lopinavir and ritonavir

WHAT IS A ROGUE INTERNET PHARMACY NETWORK?

Most illegal internet pharmacies belong to organized criminal networks, many of which have been the recipients of FDA warning letters. These networks are often complex, global operations that include hundreds – or even thousands – of related websites. The network operators create website templates and run back-end services (eg, payment processing and pharmaceutical shipping). They offer these templates and services to "affiliate marketers" who: (1) operate websites on behalf of the network; (2) drive traffic to those websites; and (3) take a small cut of the profits. Illegal pharmacy networks typically sell prescription-only drugs without requiring a prescription, sell unapproved drugs, and do not hold proper licensure in the jurisdictions where they offer shipping.

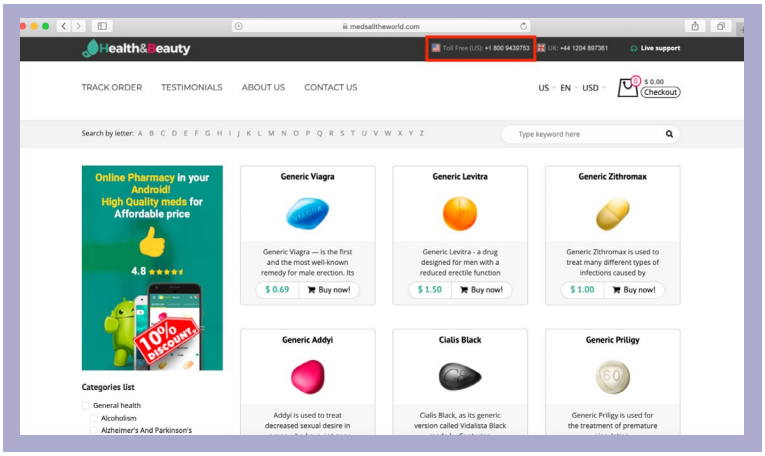
(sold together under the brand name Kaletra®) are antiretrovirals that are being tested as a possible COVID-19 treatment. NABP has also seen websites peddling diltiazem, furosemide, and mefloquine – all of which are being studied as possible coronavirus treatments. Of course, all of these treatments are unproven, and dangerous if taken without proper oversight. Because online pharmacy networks are criminal opportunists, some have even added face masks to their product lineup.

Rx-Partners, a criminal network that has been the recipient of two FDA warning letters, has created a COVID-specific template that offers patients chloroquine and "generic Kaletra."[4,5] The template also includes frightening, and wholly misleading, information about the disease. For example, it claims that COVID-19 has a 40% mortality rate. By contrast, best estimates suggest the mortality rate is below 4% globally.[6]



Rx-Partners' COVID-specific website template

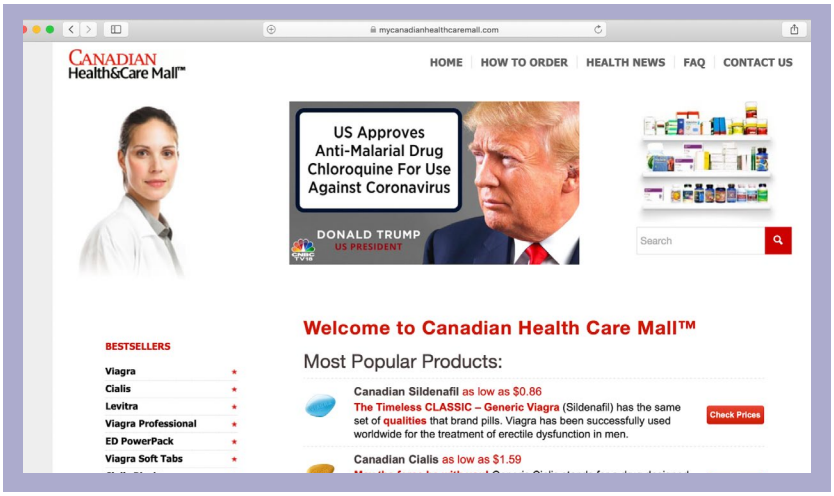
How do we know that this website is connected to the Rx-Partners network, which usually specializes in "lifestyle" drugs (eg, Viagra® and Cialis®)? There are a number of "tells" – but one obvious connection is the contact phone number, which matches the number found on many Rx-Partner websites (see example below).



Rx-Partners' website with phone number that matches their COVID-19 website

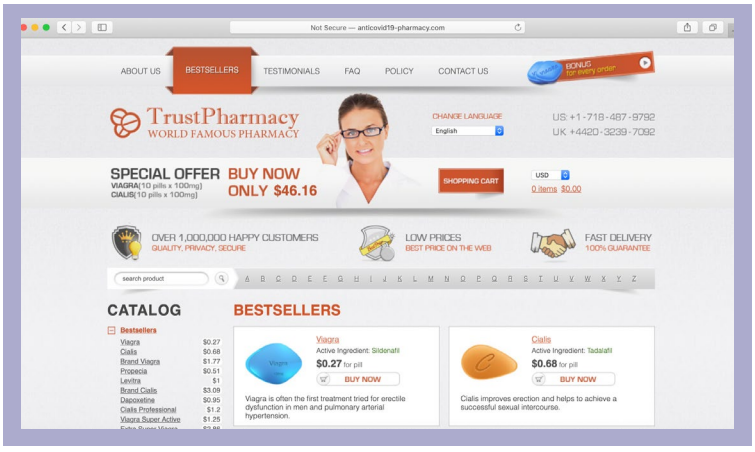
Other rogue pharmacy networks have added coronavirus-related images or content to already existing (pre-pandemic) templates. For example, the prolific EvaPharmacy network has added a photo of President Donald J. Trump to its frequently used "Canadian Health&Care Mall" template. Clicking on the image redirects users to a web page that offers chloroquine and Lopimune (an unapproved version of lopinavir/ritonavir). While rogue internet pharmacy content changes frequently, at the time of NABP's review, the website claimed that both drugs were "out of stock."

Finally, some affiliate networks have purchased domain names that include COVID-19 words and phrases, but, to date, the websites do not appear to market any COVID-specific treatments. For example, despite its name, *anticovid19-pharmacy.com* does not market any drugs as COVID-19 treatments. Instead, it uses the "TrustPharmacy" template associated with the rogue network known as PharmacyMall. Of course, the website operator may be using the TrustPharmacy template as a placeholder, as they wait for the pharmacy network to add COVID-specific content.

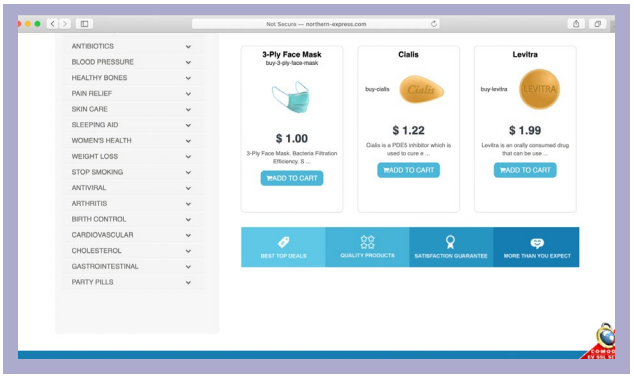


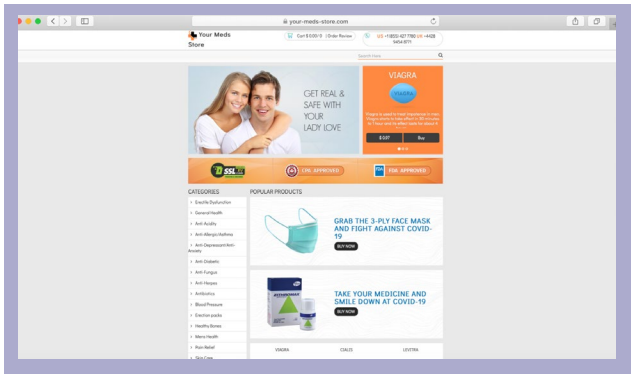
EvaPharmacy adds COVID-19 content to an existing template

It is important to remember that rogue pharmacy network operators are opportunists. They follow the money. As proof, a number of rogue pharmacy networks recently added face masks to their product lineups. This is noteworthy because face mask fraud is rampant during this pandemic.[7]



***anticovid19-pharmacy.com* does not currently sell popular COVID-19 treatments**





Examples of rogue pharmacies selling face masks

NEWLY CREATED COVID-RELATED WEBSITES SOMETIMES REDIRECT USERS TO ESTABLISHED NETWORK SITES

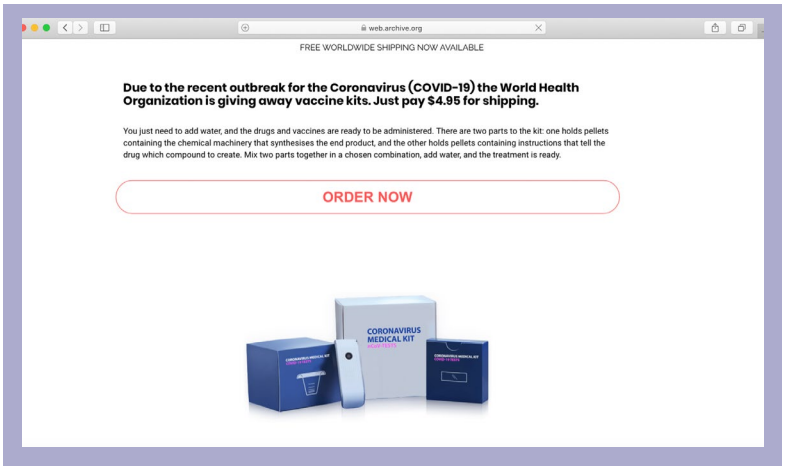
Newly created COVID-related domain names sometimes do not host independent content; instead, they redirect users to established network websites. For example, *covid19-meds.com* — which, as of the date of this report, is only a few weeks old – does not sell drugs directly. When a consumer clicks on the "COVID ANTIBIOTICS" button, the website opens a new tab, leading to *hcovid19.hellpinmeds24.net*. At the same time, the original tab automatically redirects to *canadadrugs.co/order-aralen-online-from-canada-to-usa-cheap-en.html*. While *covid19-meds.com* was created on March 23, 2020, *hellpinmeds24.net* and *canadadrugs.co* are established websites (created in May 2019 and December 2018, respectively).

MANY COVID-RELATED ROGUE PHARMACIES ARE REGISTERED WITH "SAFE HAVEN" REGISTRARS

Unsurprisingly, many COVID-related rogue pharmacies are registered with known "safe haven" registrars. For example, over 50% of the active websites identified by NABP registered their domain names with Hosting Concepts B.V., dba Openprovider. This domain name registrar is not new to regulatory scrutiny. In 2018, FDA submitted an abuse complaint under Section 3.18.2 of the 2013 Internet Corporation for Assigned Names and Numbers (ICANN) Registrar Accreditation Agreement regarding the use of domain names for illegal purposes.[8] That same year, Hosting Concepts B.V. was added to the United States Trade Representatives' "Notorious Markets List."[9]

DOMAIN NAME REGISTRATION INFORMATION FOR ALMOST ALL IDENTIFIED WEBSITES IS ANONYMIZED

Over 90% of the COVID-related domain names identified by NABP utilize anonymized domain name registration (eg, privacy/proxy services). We know that this type of anonymized data has already created difficulties for law enforcement agencies that are investigating COVID fraud. For example, in its efforts to shut down *coronavirusmedicalkit.com*, the Federal Bureau of Investigation and Department of Justice (DOJ) encountered delays related, in part, to anonymized domain name registration information. In that case, *coronavirusmedicalkit.com* offered what it fraudulently claimed were free World Health Organization (WHO) COVID-19 vaccine kits in exchange for a $4.95 "shipping charge." According to DOJ, the website was actually harvesting credit card information. The domain name was registered with Namecheap, but its domain name registration was privacy protected. Although DOJ informed Namecheap about the fraudulent statements on the website on March 19, 2020, the website was still accessible to the public as of March 21, 2020.[10,11]



An archived version of *coronavirusmedicalkit.com*, which claimed to provide free COVID-19 "vaccine kits" from WHO

GOVERNMENT ACTORS AND PUBLIC INTEREST GROUPS ARE CALLING ON INTERNET STAKEHOLDERS TO HELP STOP COVID-19 FRAUD

Government agencies, members of Congress, and state attorneys general are calling on private sector internet companies to take action against COVID-19 cybercrime. For example, New York Attorney General (AG) Letitia James sent letters to a number of domain name registrars, asking that they stop "bad actors from taking advantage of the current crisis."[12] The AG called for: (1) use of automated and human review of domain name registration and traffic patterns to identify fraud; (2) human review of complaints from the public and law enforcement about fraudulent or illegal use of coronavirus domains, including creating special channels for such complaints; (3) aggressive enforcement for the illegal use of coronavirus domains; and (4) de-registration of certain known bad actors, as well as implementing blockers that prevent rapid registration of coronavirus-related domains.[13]

Three US senators – Cory Booker, Margaret Wood Hassan, and Mazie Hirono – combined forces to ask eight domain name registrars and hosting sites to combat pandemic-related scams.[14] Specifically, the senators asked for the registrars to: "(1) exercise diligence and ensure that only legitimate organizations can register coronavirus-related domain names and domain names referencing online communications platforms; (2) act quickly to suspend, cancel, or terminate registrations for domains that are involved in unlawful or harmful activity; and (3) cooperate with law enforcement to help bring to justice cybercriminals profiting from the coronavirus pandemic."[15]

Members of the private sector are also calling for action. For example, 40 public health, trade association, industry, and research groups sent a joint letter to Vice President Mike Pence, members of the White House Coronavirus Task Force, and other state and national leaders, urging them "to require – not ask – for registrars to do more against online scams."[16]

INTERNET INTERMEDIARIES ARE TAKING ACTION

NABP notes that some domain name registrars are taking steps to prohibit bad actors from exploiting the pandemic. For example, Namecheap pledged to stop accepting the automated registration of website names that include words or phrases tied to COVID-19.[17] GoDaddy has taken action against several COVID-19 cybercriminals.[18] In Canada, Tucows is flagging all "covid" and "corona" domains for manual review and is "on the lookout in particular for any sites peddling fake COVID-19 cures or tests."[19] We also know that some internet domain providers and registrars have worked with law enforcement to disrupt hundreds of websites used to exploit the COVID-19 pandemic.[20]

On a broader level, ICANN (the multi-stakeholder group that oversees internet governance) is responding to the pandemic by pushing for access to domain name registration information. Göran Marby, the president and chief executive officer of ICANN, recently stated: "Combating abuse requires predictable and reliable access to domain name registration data for those with a legitimate interest. ICANN org continues to try to gain clarity under the European Union's General Data Protection Regulation with regard to whether a Unified Access Model for gTLD domain name registration data is possible under EU law. Access to this registration data is critical for law enforcement and security practitioners to protect Internet users from the criminals leveraging the COVID-19 pandemic, or any other threats that emerge, for fraudulent and criminal activity."[21]

NABP applauds registrars' voluntary action and ICANN's efforts to protect internet users. As a domain name registry operator and member of the ICANN community, we would be happy to assist as needed.

CONCLUSION

Rogue internet pharmacy networks are taking advantage of the pandemic and peddling unproven and dangerous prescription-only drugs to treat COVID-19. This is not surprising; these criminal networks have always preyed on vulnerable patient populations. While this behavior is predictable, the harm caused by these bad actors is largely preventable. Domain name registrars can and should voluntarily lock and suspend domain names engaged in illegal activities; they should also ensure that registration information is accurate, non-anonymous, and accessible where domain names are used commercially. Search engines can and should flag or de-index known illegal actors.

NABP calls on internet intermediaries to implement long-term policies that will not only put a stop to COVID-related cybercrime, but will also shut down rogue internet pharmacy networks for good. With respect to domain name registrars: if these entities do not take significant voluntary action, then NABP will support legislation that requires registrars to validate domain name registration information and make registration data accessible. NABP will also support legislation that requires domain name registrars to immediately lock and suspend any domain name used to facilitate COVID-19 and other public health scams.

For information about NABP's Rogue Rx: Activity Report, or the Association's research and reporting capabilities, please contact Policy and Communications Director Melissa Madigan via email at mmadigan@nabp.pharmacy.

NABP

RESOURCES

[1] Buy Safely. NABP's consumer safety website
https://safe.pharmacy/buy-safely/.
Updated May 2020. Accessed May 5, 2020.

[2] FDA. Internet Pharmacy Warning Letters.
https://www.fda.gov/drugs/drug-supply-chain-integrity/internet-pharmacy-warning-letters.
Accessed April 18, 2020.

[3] FDA. Emergency Use Authorization.
https://www.fda.gov/emergency-preparedness-and-response/mcm-legal-regulatory-and-policy-framework/emergency-use-authorization.
Accessed April 18, 2020.

[4] FDA. Warning Letter to Rx-Partners.
https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/rx-partners-09192017.
September 19, 2017. Accessed April 18, 2020.

[5] FDA. Warning Letter to Rx-Partners.
https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/rx-partners-06082015.
June 8, 2015. Accessed April 18, 2020.

[6] WHO. Q&A: Similarities and differences – COVID-19 and influenza.
https://www.who.int/news-room/q-a-detail/q-a-similarities-and-differences-covid-19-and-influenza.
March 17, 2020. Accessed April 18, 2020.

[7] Corona Crimes: Multi-Million Face Mask Scam Foiled By Police Across Europe [news release]. The Hague, the Netherlands: Europol; April 14, 2020.
https://www.europol.europa.eu/newsroom/news/corona-crimes-multi-million-face-mask-scam-foiled-police-across-europe.
Accessed May 5, 2020.

[8] FDA. Hosting Concepts B.V. d/b/a Openprovider - www.chemists-shop.com.
https://www.fda.gov/consumers/health-fraud-scams/hosting-concepts-bv-dba-openprovider-wwwchemists-shopcom.
Accessed April 18, 2020.

[9] Office of the US Trade Representative. 2018 Out-of-Cycle Review of Notorious Markets. https://ustr.gov/sites/default/files/2018_Notorious_Markets_List.pdf.
Accessed April 18, 2020.

[10] Interisle Consulting Group, LLC. Domain Name Registration Data at the Crossroads: The State of Data Protection, Compliance, and Contactability at ICANN.
http://www.interisle.net/sub/DomainRegistrationData.pdf.
March 31, 2020. Accessed April 18, 2020.

[11] US District Court, Western District of Texas. USA v. John Doe, a/k/a "*coronavirusmedicalkit.com.*" Case No. A-20-CV-306; March 21, 2020.
https://www.justice.gov/opa/press-release/file/1260126/download.
Accessed April 18, 2020.

[12] Attorney General James Asks GoDaddy and Other Online Registrars to Halt and De-list Domain Names Used for Coronavirus-Related Scams and Fake Remedies [news release]. New York, NY: New York Attorney General Letitia James; March 20, 2020.
https://ag.ny.gov/press-release/2020/attorney-general-james-asks-godaddy-and-other-online-registrars-halt-and-de-list.
Accessed April 18, 2020.

[13] Letter to Nima Kelly, Chief Legal Officer at GoDaddy, Inc. Albany, NY: State of New York Office of Attorney General; March 19, 2020.
https://ag.ny.gov/sites/default/files/3.19.20_letter_concerning_godaddy_and_coronavirus.pdf.
Accessed April 18, 2020.

[14] Hirono, Booker, Hassan Call on Domain Name Gatekeepers to Combat Coronavirus-Related Scams and Misinformation [news release]. Washington, DC: Senator Mazie K. Hirono; April 14, 2020.
https://www.hirono.senate.gov/news/press-releases/hirono-booker-hassan-call-on-domain-name-gatekeepers-to-combat-coronavirus-related-scams-and-misinformation.
Accessed April 18, 2020.

[15] Letter to Amanpal S. Bhutani, Chief Executive Officer at GoDaddy, Inc. Honolulu, HI: Senator Mazie K. Hirono; April 13, 2020.
https://www.hirono.senate.gov/imo/media/doc/2020.04.13%20Letter%20to%20GoDaddy%20re%20Coronavirus%20Domain%20Names.pdf.
Accessed April 18, 2020.

[16] Letter to Vice President Pence. Washington, DC: Alliance for Safe Online Pharmacies; April 9, 2020. https://buysaferx.pharmacy//wp-content/uploads/2020/04/Letter-to-VP-Pence-on-COVID-19-Scams-from-40-Organizations_040920.pdf. Accessed April 18, 2020.

[17] Bajak F. Internet firm restricts virus-themed website registrations. ABC News. https://abcnews.go.com/Technology/wireStory/internet-firm-restricts-virus-themed-website-registrations-69825166. March 26, 2020. Accessed April 18, 2020.

[18] Coble S. Domain Registrars Take Action Against Fraudulent COVID-19 Websites. *Infosecurity* Magazine. https://www.infosecurity-magazine.com/news/domain-registrars-combat-covid-19. March 27, 2020. Accessed April 18, 2020.

[19] Coble S. Domain Registrars Take Action Against Fraudulent COVID-19 Websites. *Infosecurity* Magazine. https://www.infosecurity-magazine.com/news/domain-registrars-combat-covid-19. March 27, 2020. Accessed April 18, 2020.

[20] Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams [news release]. Washington, DC: DOJ; April 22, 2020. https://www.justice.gov/opa/pr/department-justice-announces-disruption-hundreds-online-covid-19-related-scams. Accessed April 23, 2020.

[21] Marby G. ICANN Org's Multifaceted Response to DNS Abuse. ICANN Blog. https://www.icann.org/news/blog/icann-org-s-multifaceted-response-to-dns-abuse. April 20, 2020. Accessed April 24, 2020.