No. 19-46

IN THE
Supreme Court of the United States

U.S. PATENT AND TRADEMARK OFFICE, ET AL.,
Petitioners,

v.

BOOKING.COM B.V.,
Respondent.

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

BRIEF OF THE INTERNET COMMERCE ASSOCIATION AS *AMICUS CURIAE* IN SUPPORT OF RESPONDENT

Megan L. Brown
Counsel of Record
David E. Weslow
Ari S. Meltzer
Jeremy J. Broggi
WILEY REIN LLP
1776 K Street NW
Washington, DC 20006
(202) 719-7000
MBrown@wiley.law

February 19, 2020

Counsel for Amicus Curiae

TABLE OF CONTENTS

Page

TABLE OF CITED AUTHORITIES

Page(s)

Cases

TABLE OF CITED AUTHORITIES

TABLE OF CITED AUTHORITIES

Page(s)

TABLE OF CITED AUTHORITIES

Page(s)

Statutes

TABLE OF CITED AUTHORITIES

TABLE OF CITED AUTHORITIES

TABLE OF CITED AUTHORITIES

Page(s)

TABLE OF CITED AUTHORITIES

Page(s)

TABLE OF CITED AUTHORITIES

INTEREST OF *AMICUS CURIAE*[1]

The Internet Commerce Association ("ICA") is a non-profit organization which advocates for the rights and interests of domain name owners and related service providers. One of the ICA's missions is to participate in the development of laws and regulations pertaining to the Internet. To that end, the ICA regularly engages in activities designed to educate lawmakers, agency officials, the courts, and other stakeholders about the value of the domain name industry in improving public confidence in Internet commerce.

The ICA has a strong interest in this important case because reversal of the Fourth Circuit's decision in the manner advocated by the Government would result in the devaluation of a significant class of intellectual property assets and would eliminate an effective tool in protecting consumers from Internet-based fraud. That result would be particularly unfair to domain name owners who, in many cases, have invested large sums in establishing domain names that should be capable of obtaining trademark protection and registration. And it would likewise be harmful to consumers, who depend upon enforceable

---

[1] No counsel for a party authored this brief in whole or in part, and no person or entity other than the Internet Commerce Association, its members, or its counsel made a monetary contribution intended to fund the preparation or submission of this brief. Counsel provided timely notice to all parties of its intent to file this brief, and all parties have given their express written consent.

trademarks for purchasing confidence and for protection against Internet-based scams.

In the case below, the Fourth Circuit held that adding the top-level domain ".com" to an otherwise generic second-level domain may result in a protectable trademark "where evidence demonstrates that the mark's primary significance to the public as a whole is the source, not the product." Pet. App. 22a.[2] It also affirmed, based on uncontroverted record evidence showing that the public understands "booking.com" to refer to Respondent's corporate brand identity and not to the act of making a hotel reservation, the district court's grant of partial summary judgment finding that "booking.com" is protectable as a trademark. *Id.* at 25a; *see id.* 12a–18a.

The Government asks this Court to overturn the Fourth Circuit's decision and to establish a new, bright-line rule that adding a generic top-level domain to a generic second-level domain name can *never* result in a protectable trademark—even though the Lanham Act codifies the very test employed by the Fourth Circuit below, *see* 15 U.S.C. § 1064(3), and even though this Court's precedents have long recognized that "[t]he commercial impression of a trademark is derived from [the mark] as a whole, not

---

[2] A top-level domain is the last segment of a domain name, such as ".com," ".edu," or ".gov." A second-level domain is the second-to-last segment of a domain name, such as "google" or "supremecourt." *See* Internet Assigned Numbers Authority, *Domain Name Services*, https://www.iana.org/domains (last visited Feb. 18, 2020).

from its elements separated and considered in detail," *Estate of P.D. Beckwith, Inc. v. Comm'r of Patents*, 252 U.S. 538, 545–46 (1920). Because the unlawful change sought by the Government would undermine the intellectual property rights of domain name owners, discourage the creation and use of new top-level domain names, and harm consumers by making them more vulnerable to Internet-based scams, the ICA urges this Court to reject the Government's novel theory and to affirm the decision of the Fourth Circuit.

SUMMARY OF ARGUMENT

The Fourth Circuit should be affirmed. The court held that adding a generic top-level domain to a generic second-level domain may result in a protectable trademark where evidence demonstrates that the mark's primary significance to the public as a whole is the source, not the product. That conclusion broke no new legal ground and correctly interprets the Lanham Act. Nevertheless, the Government asks this Court to overturn the Fourth Circuit's decision and to establish a new, bright-line rule that adding a generic top-level domain to an otherwise generic second-level domain name can *never* result in a protectable trademark.

The unlawful result the Government seeks would have deleterious effects on the Internet economy as a whole and the domain name system in particular. To begin, the rule would undermine recognition of the intellectual property rights of domain name owners. Many domain name owners have heavily invested in the goodwill of their operating businesses. That

investment is made in reliance on the understanding that descriptive domain names are capable of obtaining federal trademark registration and protection where the names have acquired distinctiveness through extensive use and promotion. The unlawful rule sought by the Government would upend those settled expectations. And it would devalue registered domain names as an asset class, treating domain name owners unfairly while destroying many of the societal benefits envisioned by trademark law.

For the same reason, the Government's proposed rule would discourage investment in the generic top-level domains newly established by the Internet Corporation for Assigned Names and Numbers ("ICANN"). ICANN is the body responsible for maintaining the global domain name system, or "DNS." The DNS is the "digital phonebook" for the Internet. The National Telecommunications and Information Administration ("NTIA"), the federal expert on DNS issues, has stated that ICANN's expansion of generic top-level domains will enable beneficial "brand-focused" investment and "enhance consumer trust and choice" in the digital economy. *ICANN's Expansion of Top Level Domains: Hearing before the S. Comm. on Commerce, Sci. and Transp.*, 112th Cong. 3 (2011) (statement of Fiona M. Alexander, Associate Administrator, Office of International Affairs, NTIA), https://www.commerce.senate.gov/services/files/98C38242-C53F-438A-BB53-2D986E4BF168. The rule proposed by the Government, however, would threaten the adoption of new generic top-level domain names by declaring *ex ante* that adding a generic top-

level domain to an otherwise generic second-level domain name can *never* result in a protectable trademark. That would reduce innovation because organizations would know that regardless of their investment to create a brand identity, they would not be able to seek trademark protection.

The Government's proposed rule would also eliminate critical legal tools for combatting cybercriminals who misuse domain names for fraudulent ends. Two of the most common malicious activities involving the DNS are typosquatting and domain name hijacking. These abuses are most readily thwarted through trademark law.

Typosquatting involves the registration of a common misspelling of a domain name so a user attempting to visit a legitimate website inadvertently visits a fraudulent website. Once the user has been directed to the fraudulent website, the typosquatter may attempt to infect the user's computer with malware, or to obtain sensitive personal or financial information that the user incorrectly believes he is providing to a legitimate website.

Domain name hijacking is similar. A domain name hijacker obtains unauthorized access to the control panel for the targeted domain and changes the registration information so that the hijacker falsely appears to be the true owner of the domain name. Once in control of the domain, the hijacker may redirect visitors for malicious purposes such as infecting their computers with malware, obtaining sensitive information, or taking control of their

computers to use them in botnets or for spam distribution.

Trademark law is a critical tool for thwarting typosquatting, domain name hijacking, and other domain name abuses. Because the DNS system cannot stop such abuses on its own, domain name owners rely on trademark remedies. ICANN's Uniform Domain Name Dispute Resolution Policy ("UDRP"),[3] in particular, provides a streamlined administrative mechanism for companies to obtain the transfer of domain names that were registered and are being used in bad faith. An important prerequisite to UDRP relief, however, is a demonstration that the domain name in question is "confusingly similar to a trademark." UDRP § 4(a). Similarly, the Anticybersquatting Consumer Protection Act ("ACPA") provides a civil remedy against anyone who "in bad faith . . . registers, traffics in, or uses a domain name . . . confusingly similar to" a trademark. 15 U.S.C. § 1125(d). With these tools, the owner of a trademark can oust cybercriminals who are attempting to harm unsuspecting consumers. Because the Government's proposed rule would significantly narrow the class of domain names eligible for trademark protection, it would in many cases eliminate these critical tools for thwarting cybercriminals who misuse domain names for malicious purposes.

---

[3] The UDRP is available at https://www.icann.org/resources/pages/policy-2012-02-25-en.

ARGUMENT

I. The Government Seeks A Bright-Line Rule That Would Devalue Registered Domain Names As A Class Of Intellectual Property Assets.

The Lanham Act establishes a federal registration system for trademarks. Registration, though not required, "gives trademark owners valuable benefits." *Iancu v. Brunetti*, 139 S. Ct. 2294, 2297, 2298 (2019). Among these benefits is federal recognition that the registered marks are "the 'property' of the owner" and that "he can exclude others from using them." *Coll. Savs. Bank v. Fla. Prepaid Postsecondary Educ. Expense Bd.*, 527 U.S. 666, 673 (1999); *see also* 1 J. Thomas McCarthy, *McCarthy on Trademarks*, § 2:10 (5th ed.) ("A trademark is a property right").

Federal recognition of trademark owners' intellectual property rights has important societal benefits. The Supreme Court has explained that the "national protection of trademarks is desirable, because trademarks foster competition and the maintenance of quality by securing to the producer the benefits of good reputation." *Matal v. Tam*, 137 S. Ct. 1744, 1752 (2017) (citation omitted). In addition, national protection reduces consumers' "costs of shopping and making purchasing decisions," *Qualitex Co. v. Jacobson Prods. Co.*, 514 U.S. 159, 163–64 (1995), by helping them to more readily "distinguish among competing producers," *Park 'N Fly, Inc. v. Dollar Park & Fly, Inc.*, 469 U.S. 189, 198 (1985).

Concomitant with these benefits is the valuation of trademarks as intellectual property assets. "[T]rademarks are valuable corporate assets." Xuan-Thao Nguyen & Erik D. Hille, *The Puzzle in Financing with Trademark Collateral*, 56 Hous. L. Rev. 365, 374 (2018). Analysts attribute multibillion-dollar values to the most well-known trademarks. *See* Brand Finance, *Global 500: The Annual Report on the World's Most Valuable Brands* (2019), https://brandfinance.com/images/upload/global_500_2019_locked_4.pdf. And even the smallest companies "will have some degree of goodwill, and therefore value, in any marks they have used in commerce and properly protected." L. M. Brownlee, *Intellectual Property Due Diligence in Corporate Transactions* § 6:1 (2019). This value is felt throughout the economy. In the most recent year for which data is available, trademark-intensive industries accounted for 23.7 million jobs and $6.1 trillion in added value to the gross domestic product of the United States. U.S. Patent and Trademark Office, *Intellectual Property and the U.S. Economy* 10, 22 (2016), https://www.uspto.gov/sites/default/files/documents/IPandtheUSEconomySept2016.pdf.

The Fourth Circuit's decision rightly protects the intellectual property assets of domain name owners. Specifically, the Fourth Circuit recognized that adding the top-level domain ".com" to an otherwise generic second-level domain may result in a protectable and registerable trademark "where evidence demonstrates that the mark's primary significance to the public as a whole is the source, not the product." Pet. App. 22a. Applying that test to Respondent's attempted registration of

"booking.com," the Fourth Circuit affirmed the district court's grant of partial summary judgment finding that "booking.com" was protectable as a trademark where uncontroverted record evidence showed that the mark, taken as whole, was descriptive rather than generic and had "acquired secondary meaning" that communicated Respondent's brand identity, not the act of making a hotel reservation. Pet. App. 25a; *see id.* at 12a–18a; *accord Park 'N Fly*, 469 U.S. at 194 (explaining "descriptive" terms with "secondary meaning" "may be registered" but "[g]eneric terms are not registrable").

The Government argues for reversal based on fears that the Fourth Circuit's decision will "undermine" "fair competition" by allowing the owner of a trademarked domain name "to preclude its competitors from calling their own goods or services by their common name." Pet'r Br. 26. According to the Government, the Fourth Circuit's decision would allow federal trademark registration of any "generic.com" domain name—that is, a generic top-level domain combined with a generic second-level domain. Based on that understanding, the Government worries that the Fourth Circuit's decision will empower "individuals or entities to monopolize language by obtaining the contractual rights to 'generic.com' domain names and then leveraging those domain names into protected trademarks." *Id.* at 17–18; *see also id.* at 31–34.

The Government's fears are unfounded. To begin, the Government misreads the Fourth Circuit's opinion. The court did not hold that combination of a

generic top-level domain and a generic second-level domain automatically results in a protectable trademark, but only that it "may" result in a protectable trademark where the evidence supports such a finding. Pet. App. 22a. In fact, the Fourth Circuit expressly repudiated the straw man the Government erects here, explaining at length that "[m]erely appending .com to [a second-level domain] does not render the resulting name non-generic because the inquiry is whether the public primarily understands the term *as a whole* to refer to the source of the proffered service." *Id.* at 20a. That holding is fully consistent with the "ancient origins" of trademark law, *see Tam*, 137 S. Ct. at 1751–52, which has from the beginning recognized that "[t]he commercial impression of a trademark is derived from it as a whole, not from its elements separated and considered in detail," *Beckwith*, 252 U.S. at 545–46.

For the same reason, the Government is mistaken when it argues that the Fourth Circuit's test unwisely bestowed "additional benefits" on trademarked domain names when the domain name itself "already" provides "substantial competitive advantage" because it is assigned by contract as a unique web address. Pet'r Br. 32–33 (emphasis omitted). As the Fourth Circuit recognized, any such advantage is mitigated by the fact that "it may be more difficult for domain-name plaintiffs to demonstrate a likelihood of confusion" when the primary significance of the mark is considered as a whole. Pet. App. 25a. Moreover, by applying the test that is codified in the Lanham Act and routinely applied in registration proceedings, *see* 15 U.S.C. § 1064(3); Pet. App. 10a n.6, the Fourth Circuit merely ensured that domain names are

treated on equal footing with other kinds of marks—and not as a disfavored class of intellectual property.

The Government's argument also shortchanges the public's understanding of domain names in the Internet economy. As a general matter, consumers recognize that domain names are often associated with brands rather than with products or classes of services. Here, for example, the district court found that the public understood "booking.com" to refer to Respondent's corporate identity and not to the act of making a hotel reservation. Pet. App. 12a–18a. And that is hardly surprising because numerous case studies confirm that top-level domain names are easily recognizable identifiers helping consumers to identify the source of the goods and services in question. *See, e.g.*, ICANN, *New Generic Top-Level Domains: Case Studies*, https://newgtlds.icann.org/en/announcements-and-media/case-studies (last visited Feb. 18, 2020).

In place of the careful weighing of such evidence, the Government seeks a declaration from this Court that adding ".com" to a second-level domain name can *never* result in a protectable trademark. Such an inflexible rule would do untold damage to the intellectual property assets of domain name owners. That result would be especially unfair because many domain name owners have taken great care to register and protect their marks and have invested large sums in promoting those marks in reliance on the promise of federal protection after the domain name has acquired distinctiveness or "secondary meaning." If this Court were to adopt a per se rule against protecting certain domain names as

trademarks, that would result in a massive devaluation of the significant intellectual property assets that are trademarked domain names.

The bright-line rule sought by the Government could also damage common law trademark protection. Trademarks have been protected at common law and in equity since the Founding. *Tam*, 137 S. Ct. at 1751. And because the federal system of trademark registration "does not preempt" state-law protection, *id.* at 1753 (citation omitted), "an unregistered trademark can be enforced under state common law," *id.*[4] But the Government's theory could put that protection at risk. The case on which the Government relies for its mistaken analogy between top-level domains and corporate entity designations arose more than a half century before the Lanham Act. *See Goodyear's Rubber Mfg. Co. v. Goodyear Rubber Co.*, 128 U.S. 598 (1888); Pet. App. 18a–19a. If this Court were nevertheless to extend that decision and create the bright-line rule sought by the Government that certain domain names can never be entitled to trademark registration or common law protection, there could be serious questions as to whether this Court was seeking to disrupt the "peaceful[ ] coexist[ance]" of federal and state trademark law. *See Tam*, 137 S. Ct. at 1753. And that doubt would have a further destabilizing effect on the valuation of trademarked domain names.

In sum, the unlawful change sought by the Government would seriously undermine valuable

---

[4] An unregistered trademark may also be enforceable under federal law. *See Tam*, 137 S. Ct. at 1752 & n.1.

intellectual property rights. The resulting devaluation of domain names would harm owners who have heavily invested in the goodwill of their operating businesses and would also reduce the societal benefits envisioned by trademark law.

II. The Government's Rule Would Discourage Investment In The Internet Economy By Precluding Trademark Protection For New Types of Domain Names.

The Government's proposed rule would also discourage investment in newly established top-level domain names that are beneficial to the global digital economy and the new era of Internet governance. Domain names play a critical role in making the Internet more accessible to consumers. The DNS has been described as the "phone book" of the Internet, translating the 10- or 11-digit Internet Protocol addresses into more memorable and recognizable names. Mike Orcutt, *The Ambitious Plan to Reinvent How Websites Get Their Names*, MIT Technology Review (June 4, 2019), https://www.technologyreview.com/s/613446/the-ambitious-plan-to-make-the-internets-phone-book-more-trustworthy/. Consumers use domain names to easily navigate to websites they know and trust and to identify the origin of online communications. As such, maintaining a reliable and reputable domain name system is essential to the success of online commerce.

The expansion of the DNS is underway. ICANN, the body responsible for maintaining the global DNS, has led the charge to introduce new generic top-level

domains into the Internet's authoritative database, known as the Root Zone. *See* ICANN, *New Generic Top-Level Domains: Delegated Strings*, https://newgtlds.icann.org/en/program-status/delegated-strings (last visited Feb. 18, 2020). New generic top-level domains—such as ".homes," ".inc," ".doctor," ".law," ".bank," ".cars," ".news," ".cpa," ".ngo," and ".organic"—have proliferated as businesses seek to differentiate their online identities and improve security. *See id.* The NTIA has supported this effort, explaining to Congress that new generic top-level domains will enable "brand-focused" investment and "enhance consumer trust and choice" in the digital economy. *ICANN's Expansion of Top Level Domains: Hearing before the S. Comm. on Commerce, Sci. and Transp.*, 112th Cong. 3 (2011) (statement of Fiona M. Alexander, Associate Administrator, Office of International Affairs, NTIA), https://www.commerce.senate.gov/services/files/98C38242-C53F-438A-BB53-2D986E4BF168.

The expansion of the DNS is already yielding positive results. Some generic top-level domains set expectations for security. For example, the top-level domain ".bank" "enhances trust in the online financial system by offering a verified, more secure and easily-identifiable location on the Internet for the global banking community and the customers it serves." ICANN, *New Generic Top-Level Domains: Case Studies*, https://newgtlds.icann.org/en/announcements-and-media/case-studies (last visited Feb. 18, 2020). Other generic top-level domains enhance branding and improve commerce by making it easier to remember how to find things. *See* Domain Name Ass'n, *Domains in the Wild*,

https://inthewild.domains/ (last visited Feb. 18, 2020). Indeed, many organizations use varied top-level domains in complementary ways and, as envisioned by the NTIA when advocating for the new generic top-level domains program, innovative uses have emerged such as moving.tips, science.news, design.studio, wheels.forsale, and more. *See id.*

The rule proposed by the Government would threaten the adoption of new generic top-level domain names. Precluding trademark protection where a generic top-level domain paired with an otherwise generic second-level domain would reduce innovation and experimentation in generic top-level domains because organizations would know that regardless of their investment to create a brand identity, they would not be able to obtain trademark protection. There is no reason for this Court to mandate that result, and it should not do so.

III. The Government's Rule Would Eliminate A Critical Consumer Protection And Anti-Fraud Tool, Opening The Door To More Domain Name Abuse.

The importance of domain names to the Internet economy means that they are a prime target for malicious actors. Cybercriminals often seek to exploit domain names for fraud and the proliferation of malware. The ICA has consistently stood against misuse of domain names for intellectual property infringement and otherwise unlawful use, as set out in its Code of Conduct. *See* ICA, Code of Conduct (rev. Nov. 9, 2018), https://www.internetcommerce.org/about-us/code-of-conduct/. Enabling trademark

protection for deserving domain names, *i.e.*, those that have reached the difficult-to-obtain precipice of acquired distinctiveness for an otherwise descriptive term, fundamentally assists in preventing fraud and misuse of domain names in commerce. Without such protections being possible, it would encourage bad actors to register and use domain names corresponding to typos or confusingly similar versions of well-known domain name brands, without fear of repercussion based upon trademark law.

Trademark protection has emerged as a critical tool to thwart fraudulent activities that involve the misuse of domain names. If, as the Government urges, well-known "generic.com" domain names are unable to acquire trademark rights under any circumstances, these domain names are likely to become massive targets for abuse and fraud. As a result, consumers will find it more difficult to distinguish between legitimate domain names and copycat domain names designed to confuse them into disclosing sensitive information, purchasing counterfeit products or services, or downloading harmful viruses and spyware.

A. Cybercriminals Abuse Domain Names Through Typosquatting And Domain Name Hijacking To Perpetrate Fraud And Proliferate Malware.

Two of the most common fraudulent activities involving the DNS are typosquatting and domain name hijacking. The enforcement of trademark rights serves as an important tool for protecting consumers from these forms of domain name abuse.

Typosquatting involves the registration of a common misspelling of a domain name so a user attempting to visit a legitimate website inadvertently visits the typosquatted domain name instead. *See* Pieter Agten et al., *Seven Months' Worth of Mistakes: A Longitudinal Study of Typosquatting Abuse*, 1 (Feb. 7, 2015), https://www.ndss-symposium.org/ndss2015/ndss-2015-programme/seven-months-worth-mistakes-longitudinal-study-typosquatting-abuse/. Among the different forms of typosquatted domain names are: (1) missing-dot typos (*e.g.*, wwwexample.com); (2) character-omission typos (*e.g.*, exmple.com); (3) character-permutation typos (*e.g.*, examlpe.com); (4) character-substitution typos (*e.g.*, ezample.com where "x" was replaced by the QWERTY-adjacent "z"); and (5) character-duplication typos (*e.g.*, exammple.com). *Id.* at 2. According to one study, 477 of the 500 most popular sites on the Internet were victims of at least one malicious typosquatting domain. *Id.* at 4

Cybercriminals are constantly changing tactics. A recent form of typosquatting involves the use of the top-level domain ".cm" to mimic a legitimate ".com" website—but without the "o"—to entice unwitting visitors to websites that may bombard the users with malware alerts and other misleading messages. *See* Brian Krebs, *Omitting the "O" in .com Could Be Costly*, KrebsOnSecurity, Mar. 29, 2018, https://krebsonsecurity.com/2018/03/omitting-the-o-in-com-could-be-costly/ (last visited Feb. 18, 2020). In the first three months of 2018 alone, almost 12 million visitors fell victim to .cm typosquatting. *See id.*

Domain name hijacking, meanwhile, involves a hacker using malicious means to assume unauthorized control of a domain name. The owner of a domain name, or the registrant, must register its domain name with an ICANN-accredited registrar. Every top-level domain name is managed by a registry operator. Domain name registrars enter into agreements with registry operators to sell domain names from that registry. *See* ICANN, Agreements & Policies, https://www.icann.org/resources/pages/agreements-policies-2012-02-25-en (last visited Feb. 18, 2020). These multiple levels of responsibility for each domain name registration create a vulnerability that hackers have learned to exploit.

A common form of domain name hijacking involves an attacker gaining unauthorized access to the registrar control panel for the targeted domain name. Namecheap, *Domain Phishing and Other Security Attacks*, https://www.namecheap.com/security/domain-phishing-security-attacks-guide/ (last visited Feb. 18, 2020). Merely accessing the control panel, however, is not enough to obtain control of a domain name. Rather, the attacker must also hack the administrative email account for the domain name. *Id.* Armed with this information, the attacker can reset the control panel password, login, and steal the domain name by transferring it to another account. *Id.*

Once a domain name has been hijacked, it can be difficult to recover. ICANN has explained that

> [i]n cases where the attackers want to keep the name, domain thieves may

> alter the registration data (WHOIS) associated with a domain name, because this is the immediate, most accessible "proof." They may alter payment information. They may transfer the domain name to a new registrar: the new registrar will have information about its customer, but may not have any registration activity history. Any of these factors can make the recovery process long and trying.

ICANN, *Documentation is Key to Recovering Hijacked Domain Names* (Apr. 14, 2016), https://www.icann.org/news/blog/documentation-is-key-to-recovering-hijacked-domain-names.

Typosquatted and hijacked domain names can be used for any number of malicious purposes. ICANN tracks security threats in domain names across four categories:

- Phishing domains: These are web pages posing as a trustworthy entity like a bank or online vendor, which are used to commit financial fraud and to steal identities, among other harms.
- Malware domains: These host or spread hostile or intrusive software like Trojan software, rootkits, or ransomware, which are installed without a user's knowledge.
- Botnet command-and-control domains: These domains host communications between a set of compromised machines, known as botnets, and the machines' controller.

- Spam domains: These domains support the distribution of spam that transmits security threats such as malware and phishing pages.

ICANN, *Understanding the Domain Abuse Activity Reporting (DAAR) Monthly Report* (2019), https://www.icann.org/en/system/files/files/daar-monthly-report-04feb19-en.pdf.

Frustratingly, online criminals rapidly change tactics. "[I]t is common for [fraudulent] operators . . . to change a site's domain name ('domain name hopping') or to use multiple domain names at once to direct users to the main site." U.S. Trade Rep., *Out-of-Cycle Review of Notorious Markets* 14 n.50 (2019), https://ustr.gov/sites/default/files/2018_Notorious_Markets_List.pdf.

B. Companies Rely On Trademark Protection To Combat Domain Name Abuse.

Because the DNS system cannot stop misuses of domain names, domain name owners have come to rely on trademark protection as the primary basis for protecting consumers from Internet scams. There are two primary mechanisms for enforcing trademark rights in a domain name against typosquatters and domain name hijackers: ICANN's Uniform Domain Name Dispute Resolution Policy and civil litigation under the Anticybersquatting Consumer Protection Act.

The UDRP provides a streamlined administrative mechanism for companies to obtain the transfer of domain names that were registered and are being used in bad faith. *See* UDRP § 4(a). UDRP

proceedings are administered by third party administration services and typically take around 60 days to complete. *See* World Intellectual Property Organization, *WIPO Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP)*, https://www.wipo.int/amc/en/domains/guide/#b2 (last visited Feb. 18, 2020). As a prerequisite for availing itself of the UDRP, a domain name owner must be able to establish that it has rights in a trademark or service mark. UDRP § 4(a)(i).[5]

The Anticybersquatting Consumer Protection Act provides another means for leveraging trademark protection to stop cybercriminals. The ACPA imposes civil liability on anyone who "in bad faith . . . registers, traffics in, or uses a domain name . . . confusingly similar to" an existing trademark. 15 U.S.C. § 1125(d). The ACPA includes *in rem* procedures designed to assist domain name owners against cybersquatters who "register domain names under aliases or otherwise provide false information in their registration applications in order to avoid identification and service of process by the mark owner." H.R. Rep. No. 106-464, at 113 (1999) (Conf. Rep.).

---

[5] In addition to establishing rights in a trademark, the rightsholder must also establish that: (i) the domain name is identical or confusingly similar to the complainant's mark; (ii) the registrant has no rights or legitimate interests in respect of the domain name; and (iii) the domain name has been registered and is being used in bad faith. *See* UDRP § 4.

The Government significantly underestimates the critical role trademark protection plays in protecting consumers from Internet scams involving misuse of domain names. For example, if the domain name "booking.com" was not entitled to trademark protection, a scammer could register domain names such as "wwwbooking.com," "bookiing.com," or "booking.cm" and use those domain names to send emails asking the recipient to click a link to update their payment information to avoid a future reservation being canceled. The link would direct the user to a malicious website where the scammer— not booking.com—would collect the payment information from the unsuspecting user. Or the scammer can create a website accessible at the closely related domain names that would distribute malware to users who mistype the authentic domain name. Worse yet, if the scammer can gain access to booking.com's administrative email account, it can steal the booking.com domain name, transfer the domain name to an overseas registrar that may not cooperate with efforts to quickly restore the domain name, and while the domain name is stolen, redirect the domain name to the hacker's own website and mail servers, allowing him to intercept email communications and web traffic intended for booking.com.

Such scenarios are not hypothetical. They reflect the reality for domain name owners today.

For example, in 2004, Central Source LLC, a joint venture of the United States' three major credit reporting agencies, announced the launch of annualcreditreport.com to provide consumers with a

secure means to request and obtain a free credit report once every 12 months in accordance with the Fair and Accurate Credit Transactions Act, 15 U.S.C. § 1681j. Consumers visiting annualcreditreport.com are required to provide personal information to validate their identity before receiving their free annual credit reports. Almost immediately, fraudsters began registering typosquatted domain names that used forms of annualcreditreport.com to entice unsuspecting Internet users to their sites. Central Source has filed numerous lawsuits under the ACPA to disable hundreds of these sites and protect consumers. *See Central Source LLC v. annaulcreditreports.com*, No. 20-CV-84 (E.D. Va.); *Central Source LLC v. annualcreditreportmonitoring.com*, No. 18-CV-453 (E.D. Va); *Central Source LLC v. Annalcreditreport.co*, No. 18-CV-1316 (E.D. Va); *Central Source LLC v. afreeannualcreditreport.com*, No. 17-CV-581 (E.D. Va.); *Central Source LLC v. freeannualcfreditreport.com*, No. 17-CV-63 (E.D. Va.); *Central Source LLC v. freeannualcreditreport2014.com*, No. 16-CV-465 (E.D. Va.); *Central Source LLC v. annuslcreditreport.com*, No. 14-CV-302, (E.D. Va.); *Central Source LLC v. annualcreditfreport.com*, No. 14-CV-303 (E.D. Va.); *Central Source LLC v. annualdcreditreport.com*, No. 14-CV-304, (E.D. Va.); *Central Source LLC v. annualcreditreport-com.us*, No. 14-CV-305 (E.D. Va.); *Central Source LLC v. aabbualcreditreport.com*, No. 14-CV-918 (E.D. Va.); *Central Source LLC v. aniualcreditreport.com*, No. 14-CV-1345 (E.D. Va.); *Central Source LLC v. anmnualcreditreport.com*, No. 14-CV-1754 (E.D. Va.); *Central Source LLC v. annualcrsditreport.com*, No.

14-CV-1755 (E.D. Va.); *Central Source LLC v. annualcredireport.org*, No. 15-CV-1038 (E.D. Va); *Central Source LLC v. annaulcrditreport.com*, No. 15-CV-1271 (E.D. Va).

Another example of typosquatting involves business cards. Clickbusinesscards.com launched in 1996 as the first company in the world to allow ordering of business cards online. When a notorious typosquatter registered the nearly identical domain name "clickbuisnesscards.com"—transposing the "i" and the "s" in "business"—the owner of clickbusinesscards.com commenced an action under the UDRP. Although the administrative panel considered the generic nature of the words "click," "business," and "cards," because the registrant had established trademark rights in the mark as whole, it was able to prevail and obtain a transfer of the typosquatted mark. *See FHG Holdings Pty Ltd d/b/a Click Business Cards v. DOMIBOT*, D2006-0669 (WIPO Aug. 1, 2006).

The ACPA has also been successfully employed to stop domain name hijacking. In 2016, International Data Communications Ltd., an information technology service provider based in Gibraltar, discovered that its domain name, 21.com, was resolving to an unauthorized website. Although the company's domain name registrar determined that its domain name management account had likely been compromised, there was nothing the registrar could do because the domain name had already been transferred to a domain name registrar in China that is a common destination registrar for stolen domain names. However, because International Data

Communications had trademark rights in 21.com, it was able to obtain a preliminary injunction and recover its 21.com domain name in less than three weeks, mitigating the harm both to the company's business and persons using 21.com. *See Int'l Data Commc'ns Ltd. v. Doe*, No. 16-CV-613-LMB-LFA (E.D. Va. June 2, 2016).

In January 2017, Flying Nurses International LLC discovered that the website and email associated with its domain name—"flyingnurse.com"—had suddenly and inexplicably stopped operating. Calls to the company's domain name service provider revealed that the domain name had been transferred to another user and then to an overseas registrar without Flying Nurses' authorization. By filing a lawsuit under the ACPA based on trademark rights in the flyingnurse.com domain name, Flying Nurses was able to recover its stolen domain name within days, substantially mitigating the harm to Flying Nurses' business and its clients. *See Flying Nurses Int'l LLC v. flyingnurse.com*, No. 17-CV-168-LMB-MSN (E.D. Va. Dec. 3, 2017).

And there are many more such cases. *See, e.g.*, *Du v. BSH.com*, No. 17-CV-698 (E.D. Va. Jan. 8, 2018) (recovery of stolen BSH.com domain name through *in rem* ACPA litigation); *Muscle Mass, Inc. v. Doe*, No. 17-CV-33 (E.D. Va. Apr. 25, 2017) (recovery of stolen musclemass.com domain name through *in rem* ACPA litigation); *GMF, Inc. v. Doe*, No. 17-CV-34 (E.D. Va. June 8, 2017) (recovery of stolen GMF.com domain name through *in rem* ACPA litigation).

These examples show the importance of preserving the possibility of establishing trademark rights in domain names. Indeed, in numerous cases, the administrative panels under the UDRP have refused to award the return of allegedly stolen generic domain names where the original owners have not been able to establish trademark rights in the domain names. *See, e.g.*, *Donald Williams v. wangyan hong / wang yan hong*, FA1605001674326 (ADR Forum June 28, 2016) (finding that complainant had no trademark rights in 5285.com); *Lingjia Cai, Yongfang Xiang v. Maolin Zhang*, D2017-0289 (WIPO Apr. 6, 2017) (declining to transfer 74 stolen domain names where complainant failed to prove it had acquired trademark rights in the names).

C. Non-Trademark Remedies Do Not Provide A Sufficient Means For Combatting Domain Name Abuse.

The Government suggests that trademark protection for domain names is not critical because other areas of law are sufficient to protect domain name owners and consumers from domain name abuse. Pet'r Br. 34–35. That position reflects a gross misunderstanding of the challenges plaguing the DNS. As noted above, the ACPA, which is the primary law used to protect consumers from misuse of domain names, requires trademark rights as an element of any claim. Similarly, the UDRP process provides for the protection of trademarks. Thus, the Government's position would substantially weaken the strongest remedy available against domain name abuse.

Contrary to the Government's suggestion, unfair competition laws are not a substitute for the ability to assert trademark rights. Pet'r Br. 35. Most ACPA cases involve defendants who are either unknown or who are outside the jurisdiction of the U.S. courts. Indeed, when it adopted the ACPA, Congress recognized that the *in rem* procedure was necessary "to respond to the problems faced by trademark holders in attempting to effect personal service of process on cyberpirates," who frequently utilize fictitious names or offshore addresses. H.R. Rep. No. 106-464, at 114. In the flyingnurse.com case discussed above, after obtaining a preliminary injunction returning the domain name based on trademark rights in the domain name, it took Flying Nurses almost 18 months and subpoenas to numerous third party registrars, Internet service providers, and email service providers to discover the full scope of the theft and amend its complaint accordingly. It would cause unthinkable harm to companies and consumers if fraudulent domain name activity could continue for even close to this long because the owner of a "generic.com" domain name was unable to assert trademark rights in its domain name.

CONCLUSION

The decision of the Fourth Circuit should be affirmed.

Respectfully submitted,

Megan L. Brown
Counsel of Record
David E. Weslow
Ari S. Meltzer
Jeremy J. Broggi
WILEY REIN LLP
1776 K Street NW
Washington, DC 20006
(202) 719-7000
MBrown@wiley.law

Counsel for Amicus Curiae

February 19, 2020