WEB OF DECEPTION: HOW CYBERSQUATTING AND FRAUDULENT ENTITIES CHALLENGE CONSUMER PROTECTION LAWS

JACOB A. DAVIS[*]

I. INTRODUCTION

From Nike to Netflix, we place our trust in brands and companies that have earned our confidence. But what if that trusted company is not what it appears? Every day, individuals are victims of fraud and deception, as scammers replicate legitimate brands or create entirely counterfeit entities to exploit unsuspecting consumers. This is the reality of cybersquatting and fraudulent business entity creation ("FCEs"), where bad faith actors exploit reputable brands for profit. These deceptive practices not only mislead consumers but can also inflict significant financial and reputational damage on legitimate businesses—and they are on the rise.

Take, for instance, a rising tech company called "NovaLens" that specializes in smart glasses. Before the company can register its ideal domain, an opportunist secures the URL "novalens.tech" and demands an outrageous price to transfer ownership. Meanwhile, another opportunist registers with "NovaLens Technologies Inc." in multiple states' respective Secretary of State offices, exploiting the name recognition built by the legitimate company to sell low-quality imitation products and deceive consumers into thinking they are purchasing from the authentic NovaLens brand. To address the challenges posed by deceptive digital practices, the legal landscape surrounding cybersquatting and FCEs has evolved; however, are these laws constitutional and sufficient to protect modern-day businesses and customers?

---

[*] J.D. Candidate, Northern Kentucky University Salmon P. Chase College of Law, 2026; Master of Music, The University of Akron, 2021; Bachelor of Music, Northern Kentucky University, 2019. I would like to thank my supervising professor, Danielle J. Lewis, and the editors of the Northern Kentucky Law Review for their resourceful advice and guidance for this project. Lastly, I am forever grateful for my family's encouragement and support throughout my legal journey.

Business entities face constant threats of deception.[1] Specifically, bad faith actors looking to steal and actively deceive newly formed or existing entities.[2] Among these concerns is cybersquatting, which involves the registration, sale, or use of an entity's domain name with the intent to profit from the goodwill of someone else's trademark.[3] Domain names, such as "ford.com," are web addresses that are assigned to businesses and individuals on the Internet.[4] To consumers, these domain names function like trademarks because they identify a source of goods or services.[5]

Typically, cybersquatters try to sell a pre-existing or variation of a domain name to the legitimate trademark owner at an inflated price. In response, the legitimate owner may be forced to capitulate because the cybersquatter's similar domain name could undermine the brand's integrity.[6] This practice creates confusion among consumers, eroding consumer trust in a brand, and complicates the enforcement of intellectual property rights.[7] Online consumers often struggle to differentiate an authentic website from a fraudulent one, as the only indicators of the site's origin and legitimacy are the website's visual design and web address.[8] Recently, however, the scope of deceptive practices has expanded.[9] FCEs have emerged and involve the formation of business entities, like corporations or limited liability companies ("LLCs"), for deceptive purposes, such as evading legal obligations, perpetrating fraud, or concealing true ownership.[10]

This Note argues that, through cybersquatting and FCEs, deceptive and bad faith practices are increasingly affecting modern entities and consumers. While existing legal frameworks attempt to address these issues, they remain inadequate; and therefore, expanding these frameworks is essential to effectively combat these challenges. Part II explores the

---

[1] *National Small Business Week: IRS Warns Entrepreneurs to Take Precautions on Data Security; Protect Their Businesses, Employees, Customers*, IRS (May 1, 2024), https://www.irs.gov/newsroom/national-small-business-week-irs-warns-entrepreneurs-to-take-precautions-on-data-security-protect-their-businesses-employees-customers [hereinafter *National Small Business Week*].
[2] *Id.*
[3] DEBORAH E. BOUCHOUX, INTELLECTUAL PROPERTY: THE LAW OF TRADEMARKS, COPYRIGHTS, PATENTS, AND TRADE SECRETS 144 (4th ed. 2012).
[4] Congress has defined "domain name" as "any alphanumeric designation that is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet." 15 U.S.C. § 1127.
[5] BOUCHOUX, *supra* note 3, at 145.
[6] *Id.* at 147.
[7] *Id.*
[8] David S. Magier, *Tick, Tock, Time Is Running Out to Nab Cybersquatters: The Dwindling Utility of the Anticybersquatting Consumer Protection Act*, 46 IDEA 415, 416 (2006).
[9] BOUCHOUX, *supra* note 3, at 147.
[10] *National Small Business Week*, *supra* note 1.

historical evolution of virtual fraud and deception, emphasizing cybersquatting and FCEs. It will cover the legal standards, requirements, relevant case law, and statutes governing cybersquatting and FCEs.

Part III advances this Note's argument that existing legal frameworks are inadequate in addressing the rise of cybersquatting and FCEs and must be expanded to combat these deceptive and bad faith practices effectively. It examines key indicators of bad faith in these schemes, their expansion into domain name creation and business entity formation, and the shortcomings of current regulations. Additionally, it evaluates federal measures and technologies, emphasizing the need for stronger legal protections to safeguard businesses and consumers. Without targeted legal reform and consistent enforcement, cybersquatting and FCEs will continue to exploit gaps in the regulatory framework, leaving businesses and consumers vulnerable to increasingly sophisticated forms of deception.

II. HISTORICAL DEVELOPMENT

A. Cybersquatting

The rise of the Internet created new ways to infringe property rights, and chief among them is cybersquatting.[11] Cybersquatting is a malicious activity where opportunists register domain names that are similar to an entity's online trademarked name with the intent to profit from the confusion and misuse of that entity's property rights.[12] For example, though Nike uses "nike.com," I could create a website called "nikedeals.com" to mimic Nike's branding, I could deceive consumers into thinking my site is an official retailer, allowing me to profit from their mistaken trust in Nike's hard-earned brand value. This practice embodies both deception and bad faith, as cybersquatters seek to exploit the reputation and goodwill of trademark holders for financial gain.[13]

Typically, cybersquatters either ransom the domain name back to the trademark holder or divert business from the trademark holder to the domain name holder.[14] Prevailing legal protections requires a showing of bad faith intent to profit from the use of a domain name that is identical or confusingly similar to a distinctive or famous mark.[15]

---

[11] Steven R. Borgman, *The New Federal Cybersquatting Laws*, 8 TEX. INTELL. PROP. L.J. 265, 266-67 (2000).
[12] *Id.*
[13] *See* STEPHEN ELIAS, PATENT, COPYRIGHT, AND TRADEMARK 355 (3d ed. 1999).
[14] *See id.* at 351.
[15] *See id.* at 350.

i. Overview and Types of Cybersquatting

Presently, there are four common forms of cybersquatting: typosquatting, identity theft, name jacking, and reverse-cybersquatting.[16] First, typosquatting involves registering domain names that are intentional misspellings of famous trademarks or names to divert internet traffic.[17] Typosquatting targets web users who enter a website address incorrectly into their browser.[18] For instance, typing "Gooogle.com" instead of "Google.com", or typing "www.amazon.co" instead of "www.amazon.com". Typosquatters use these fake websites to compel legitimate website owners to buy the cybersquatting domain names, generate increased "web traffic" to their sites, which may contain advertisements or links that generate revenue for the cybersquatter, or spread malware.[19]

Second, identity theft describes crimes where someone unlawfully obtains and uses another individual's private data to involve deception or fraud, usually for financial gain.[20] In cybersquatting, these identity thieves steal and create domains with your personal information.[21] For example, cybersquatters may buy a domain that was inadvertently not renewed by the previous owner.[22] After registering expired domain names, cybersquatters may link them to duplicates of the previous domain owners' websites.[23] As a result, cybersquatters will trick visitors into their websites, thinking they are visiting the actual websites of the previous domain owners.[24]

Third, name-jacking is when someone registers a domain name associated with an individual's name, usually a celebrity or a well-known public figure.[25] For example, if a celebrity like Taylor Swift has an official website at "taylorswift.com," but an opportunist registers "taylorswiftonline.com" and fill it with ads or misleading content, the opportunist could profit from the web traffic of fans who mistakenly visit the fake site, believing it to be affiliated with her. These "name-jackers" profit from the web traffic related to the individuals being targeted.[26]

---

[16] Jonathan H. Gatsik, *Cybersquatting: Identity Theft in Disguise*, 35 SUFFOLK U.L. REV. 277, 290 (2001); *see also* BOUCHOUX, *supra* note 3, at 150.
[17] BOUCHOUX, *supra* note 3, at 150-51.
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.* at 150-51.
[23] BOUCHOUX, *supra* note 3, at 152.
[24] *Id.*
[25] *Id.* at 150.
[26] *Id.* at 151.

Lastly, reverse cybersquatting is an aggressive action that a cybersquatter uses to obtain a specific domain name on the Internet.[27] Reverse cybersquatters try to secure a domain name that is legitimately owned by someone else through intimidation and pressure to transfer ownership.[28] The following legal protections specifically combat these four forms of cybersquatting.

ii. Legal Protections

The Internet has dramatically changed communication.[29] However, as discussed above, this change has also brought conflict over the use of domain names and trademarks. The assignment of domain names, or web addresses, has resulted in disputes between the fraudulent owners of domain names and the owners of trademarks.[30] The U.S. Department of Commerce first addressed this issue under the Internet Corporation for Assigned Names and Numbers ("ICANN") in 1998 to coordinate naming policies.[31]

ICANN, a nonprofit public benefit corporation, was influenced by the U.S. Department of Commerce's "White Paper," which proposed the establishment of a private, not-for-profit corporation to manage the domain name system.[32] The White Paper emphasized the need for a balanced representation of various stakeholders in the Internet community and aimed to ensure the stability and security of the domain name system.[33] Since 1998, ICANN has assumed responsibility for overseeing the domain name system in the United States.[34]

To further combat these issues, Congress has responded with various legislative frameworks to address cybersquatting. If a victim of cybersquatting, a potential plaintiff has several options: (1) An action for trademark infringement, if the likelihood of confusion and use in commerce can be shown, (2) An action under the federal dilution statute, (3) A civil suit under the Anti-Cybersquatting Consumer Protection Act ("ACPA"), or (4) An administrative quasi-arbitration proceeding through ICANN's

---

[27] *Id.*
[28] BOUCHOUX, *supra* note 3, at 151.
[29] Jonathan M. Ward, *The Rise and Fall of Internet Fences: The Overbroad Protection of the Anticybersquatting Consumer Protection Act*, 5 MARQ INTELL. PROP. L. REV. 211, 212 (2001).
[30] *Id.* at 212.
[31] ICANN is governed by an international board of directors elected in part by various members of the Internet community. *The ICANN History Project,* ICANN, https://www.icann.org/history (last visited Oct. 4, 2024).
[32] 5 Anne Gilson LaLonde, Gilson on Trademarks § 30.08 (Matthew Bender & Co. 2024); s*ee also* NAT'L TELECOMM. & INFO. ADMIN., *STATEMENT OF POLICY ON THE MANAGEMENT OF INTERNET NAMES AND ADDRESSES* (June 10, 1998), https://www.ntia.gov/federal-register-notice/statement-policy-management-internet-names-and-addresses.
[33] Anne Gilson LaLonde, *supra* note 32.
[34] ICANN*, supra* note 31.

dispute resolution process, the Uniform Domain-Name Dispute-Resolution Policy ("UDRP").[35] Since 1999, cybersquatting is mostly addressed under the ACPA and UDRP.[36]

The ACPA, passed in 1999, addresses this issue in the United States.[37] Internationally, the UDRP provides another framework.[38] Under both the ACPA and UDRP, trademark holders can seek remedies by proving that cybersquatters acted with bad faith intent to profit from the use of a domain name that is identical or confusingly similar to their distinctive or famous mark.[39] Both of these frameworks provide a mechanism for trademark owners to reclaim their domain names and seek damages for the harm caused by cybersquatters.[40]

1. Anti-Cybersquatting Consumer Protection Act of 1999

In the early days of the Internet, trademark owners had limited recourse against cybersquatting and deceptive practices.[41] But on November 29, 1999, Congress enacted the ACPA, which offers a greater level of protection for trademark owners.[42] The ACPA addresses cybersquatting by targeting those who register domain names in bad faith to profit from the goodwill associated with the trademarks of others.[43] The ACPA is designed to protect consumers and businesses from the abusive registration of distinctive marks as domain names, thereby promoting the growth of online commerce and providing clarity in the law for trademark owners.[44]

The ACPA creates a cause of action against anyone who, with bad faith intent to profit from a mark, registers, traffics in, or uses a domain name that is identical or confusingly similar to a distinctive or famous mark.[45] This legislative measure was necessary because cybersquatters had become increasingly sophisticated and were able to insulate themselves from liability under previous laws, such as the Federal Trademark Dilution Act.[46]

2. Uniform Domain-Name Dispute-Resolution Policy

Working in tandem with the ACPA, the UDRP provides a quicker and less expensive alternative for resolving domain name disputes without

---

[35] BOUCHOUX, *supra* note 3, at 150-51.
[36] *Id.*
[37] *Id.* at 149.
[38] *Id.*
[39] *Id.*
[40] BOUCHOUX, *supra* note 3, at 150-51.
[41] Ward, *supra* note 29, at 211, 216.
[42] *Id.* at 223.
[43] ELIAS, *supra* note 13, at 334.
[44] *Id.* at 334-36.
[45] *Id.*
[46] Ward, *supra* note 29, at 212, 222.

resorting to court action.[47] In 1999, after assuming control of the domain name registration process, ICANN adopted the UDRP, an international policy for resolving controversies relating to domain names.[48] All ICANN-accredited registrars must follow UDRP, and ICANN has designated five approved providers to oversee disputes.[49] Of the five, the World Intellectual Property Organization ("WIPO"), headquartered in Geneva, has emerged as the most popular forum for domain name disputes.[50] The UDRP establishes an administrative procedure for efficient and inexpensive resolution of a specific category of disputes: those arising from abusive, bad faith registrations of domain names, namely, cybersquatting.[51]

Under the UDRP, a trademark holder files an online complaint with one of the approved dispute resolution service providers.[52] These providers set their own fees, which average about $1,500.[53] There is no discovery and no personal appearances; everything is done via paper or electronic filing.[54] [55] Remedies are limited to canceling a wrongful domain name or transferring it to its rightful owner.[56] Neither monetary damages nor injunctive relief can be obtained under the UDRP.[57] Nevertheless, if the trademark owner seeks a quick and inexpensive resolution of a domain name dispute, the UDRP provides an excellent forum for the cancellation or transfer of a domain name.[58]

The case *Sallen v. Corinthians Licenciamentos LTDA* illustrates the interaction between the UDRP and ACPA in addressing cybersquatting disputes.[59] Sallen, a U.S. resident, registered the domain name "corinthians.com", which was challenged by Corinthians Licenciamentos LTDA ("CL"), a Brazilian company associated with the Corinthians soccer team.[60] The dispute was submitted to the WIPO under the UDRP, which ruled against Sallen, finding him to be a cybersquatter and ordering the domain's transfer to CL.[61] In response, Sallen sought relief in U.S. federal court, arguing that his registration did not violate the ACPA and that he

---

[47] BOUCHOUX, *supra* note 3, at 151.
[48] The UDRP took effect at the beginning of 2000. Ward, *supra* note 29, at 229.
[49] *Id*.
[50] *Id.* at 230.
[51] *Id.*
[52] BOUCHOUX, *supra* note 3, at 151.
[53] *Id.* at 150-51.
[54] *Id.*
[55] A decision is usually rendered by a neutral arbitration panel, either a single or three-membered panel, in about two months. *Id.*
[56] *Id.*
[57] BOUCHOUX, *supra* note 3, at 149-52.
[58] *Id.*
[59] Sallen v. Corinthians Licenciamentos LTDA, 273 F.3d 14, 16 (1st Cir. 2001).
[60] *Id.* at 15-16.
[61] *Id.* at 16.

should not be required to transfer the domain name.[62] The First Circuit emphasized the ACPA's role in providing domain name registrants a judicial remedy to challenge UDRP decisions and held that 15 U.S.C. § 1114(2)(D)(v) of the ACPA allowed Sallen to seek an injunction to retain the domain name, if he could demonstrate compliance with the law.[63]

Sallen highlights the dual approach of the ACPA and UDRP in balancing between protecting trademark holders from cybersquatting and ensuring domain name registrants have legal recourse against potentially overreaching trademark claims. This ruling underscored the distinction between the UDRP, which serves as an administrative dispute resolution mechanism, and the ACPA, which grants federal courts the authority to override UDRP decisions.

iii. The Legal Standards and Elements

To establish a claim under either ACPA or UDRP, several key elements must be met. The ACPA and WIPO processes serve similar purposes but operate within different legal frameworks. The ACPA provides a statutory cause of action and WIPO offers an administrative resolution. The UDRP requires the trademark owner to prove: (1) The allegedly wrongful domain name is identical or confusingly similar to the complainant's trademark, (2) The domain name registrant has no legitimate interest in the domain name, and (3) The domain name was registered and is being used in bad faith.[64]

Similarly, ACPA asks that a plaintiff demonstrate: (1) The defendant registered, trafficked in, or used a domain name; (2) The domain name is identical or confusingly similar to a protected mark owned by the plaintiff; and (3) The defendant acted with bad faith intent to profit from that mark.[65] The ACPA provides a non-exhaustive list of factors that courts may consider in determining whether a defendant acted with bad faith intent to profit.[66] Cybersquatting is mostly addressed by the ACPA, which allows trademark owners to seek damages and other remedies against cybersquatters.[67] The key element for a successful claim under the ACPA is proof of a bad faith intent to profit from the mark.[68] This requirement

---

[62] *Id.*
[63] *Id.* at 26.
[64] *See* BOUCHOUX, *supra* note 3, at 149-52.
[65] *Id.* at 149*; see* Prudential Ins. Co. of Am. v. Shenzhen Stone Network Info. Ltd., 58 F.4th 785 (4th Cir. 2023).
[66] Aviva United States Corp. v. Vazirani, 902 F. Supp. 2d 1246 (D. Ariz. 2012), *aff'd*, 632 F. App'x 885 (9th Cir. 2015).
[67] Stephens v. Trump Org. LLC, 205 F. Supp. 3d 305, 308-309 (E.D.N.Y. 2016).
[68] *Id.* at 313.

ensures that the ACPA targets only the specific evils that Congress sought to prevent, thereby limiting the statute's scope.[69]

In either case, a plaintiff must first demonstrate that they have a valid trademark entitled to protection. They must also show that the trademark is distinctive or famous enough to make an ACPA claim.[70] This may require proving that the mark is registered, distinctive, or has acquired distinctiveness, and if claiming fame, that it is widely recognized by the general public.[71] For example, "Simply Lemonade" could demonstrate its mark is registered, inherently distinctive, or has acquired distinctiveness through long-term use and consumer recognition.[72] If claiming fame, Simply Lemonade could show that the mark was widely recognized by the general public, using evidence like sales data, advertising reach, and media coverage.[73] These requirements ensure that only marks with a certain level of recognition and legal protection can be the basis for a cybersquatting claim.[74]

Next, the plaintiff must show that the defendant's domain name is identical or confusingly similar to the plaintiff's mark.[75] This element focuses on the likelihood of consumer confusion or dilution of the mark's distinctiveness.[76] In *People for Ethical Treatment of Animals v. Doughney (PETA)*, the Fourth Circuit ruled that "peta.org" was confusingly similar to PETA's mark, emphasizing that an internet user would not realize they were not on an official PETA website until after accessing peta.org, even though the site was a parody.[77] Courts typically compare the defendant's domain name with the plaintiff's trademark to determine if they are identical or

---

[69] Way Int'l v. Church of the Way Int'l, No. 7:15-CV-370-RDP, 2017 U.S. Dist. LEXIS 13736, at *22 (N.D. Ala. Feb. 1, 2017).
[70] BOUCHOUX, *supra* note 3, at 149.
[71] A mark obtains a secondary meaning—and therefore acquires distinctiveness—when, in the minds of the relevant consuming public, the "primary significance of the term . . . is not the product but the producer." Royal Palm Props., Ltd. Liab. Co. v. Pink Palm Props., Ltd. Liab. Co., 950 F.3d 776, 784 (11th Cir. 2020) (quoting Am. Television & Communs. Corp. v. Am. Communs. & Television, Inc., 810 F.2d 1546, 1549 (11th Cir. 1987)).
[72] Lovely Skin, Inc. v. Ishtar Skin Care Prods., LLC, 745 F.3d 877, 888 (8th Cir. 2014).
[73] *Id.*
[74] HER, Inc. v. RE/MAX First Choice, LLC., 468 F. Supp. 2d 964, 972 (S.D. Ohio 2007); *see* Holding Co. of the Vills., Inc. v. Worthmann LLC, No. 5:22-cv-269-GAP-PRL, 2023 U.S. Dist. LEXIS 108119 (M.D. Fla. June 22, 2023); *see also* Facebook Inc. v. Namecheap Inc., No. CV-20-00470-PHX-GMS, 2020 U.S. Dist. LEXIS 210068 (D. Ariz. Nov. 10, 2020).
[75] BOUCHOUX, *supra* note 3, at 149.
[76] The ultimate question is "whether relevant consumers are likely to believe that the products or services offered by the parties are affiliated in some way." *HER, Inc*., 468 F. Supp. 2d at 978 (quoting Daddy's Junky Music Stores Inc. v. Big Daddy's Family Music Center, 109 F.3d 275, 280 (6th Cir. 1997)).
[77] People for Ethical Treatment of Animals v. Doughney, 263 F.3d 359, 369 (4th Cir. 2001).

confusingly similar.[78] However, this requirement does not involve examining the content of the defendant's website.[79]

Furthermore, courts have been generous in finding confusing similarities, making it a relatively low hurdle for mark owners.[80] Even if a domain name was registered in good faith or is not necessarily confusingly similar, the mark owner might still claim that the domain name or website is likely to confuse users into believing it is sponsored or endorsed by the mark owner, potentially leading to an infringement claim under traditional trademark law.[81]

Additionally, the phrase "confusing similarity" under the ACPA holistically means that the plaintiff's mark and the defendant's domain name are so similar in sight, sound, and meaning that they could be confused.[82] For instance, if a company owns the mark "TechNova", and someone registers the domain "TekNova.com". Here, the two are so similar in sight, sound, and meaning that consumers could easily confuse them. Courts generally hold that a domain name incorporating a trademark is confusingly similar if it bears such a visual resemblance that internet users would reasonably assume the names were modified, used, approved, and/or permitted by the plaintiff.[83] Slight differences, such as the addition of minor or generic words, are irrelevant in assessing confusing similarity.[84] Misspellings of trademarks and domain names mimicking the name of a trademark owner's legitimate website are also considered confusingly similar.[85] The fact that confusion could be resolved by visiting the website is not relevant to whether the domain name itself is identical or confusingly similar to the plaintiff's trademark.[86]

Lastly, a plaintiff must prove that the defendant acted with bad faith intent to profit from that mark.[87] Bad faith intent to profit from a trademark is a key element for a trademark owner to prove.[88] This is because it distinguishes malicious and exploitative conduct from legitimate domain name registration and use.[89] After all, the primary purpose of the ACPA is

---

[78] AMF Inc. v. Sleekcraft Boats, 599 F.2d 341, 348-49 (9th Cir. 1979) (detailing the factors courts consider when analyzing the likelihood of confusion); *see HER, Inc*., 468 F. Supp. 2d at 971.
[79] *HER, Inc.*, 468 F. Supp. 2d at 972.
[80] Boigris v. EWC P&T, LLC, 7 F.4th 1079, 1089 (11th Cir. 2021).
[81] Toyota Motor Sales, U.S.A., Inc. v. Tabari, 610 F.3d 1171, 1176 (9th Cir. 2010).
[82] *Boigris*, 7 F.4th at 1089.
[83] *Id.* (quoting Omega S.A. v. Omega Eng'g, Inc., 228 F. Supp. 2d 112, 127 (D. Conn. 2002)).
[84] BOUCHOUX, *supra* note 3, at 149.
[85] *Id.*
[86] *Id.* at 555.
[87] Stephens v. Trump Org. LLC, 205 F. Supp. 3d 305, 308 (E.D.N.Y. 2016).
[88] Gioconda Law Grp. PLLC v. Kenzie, 941 F. Supp. 2d 424, 431 (S.D.N.Y. 2012).
[89] Soter Techs., LLC v. IP Video Corp., 523 F. Supp. 3d 389, 402-03 (S.D.N.Y. 2021).

to protect trademark owners from those who seek to unfairly benefit from the goodwill and reputation associated with their marks.[90] It is not intended to stifle legitimate competition or restrict the fair use of domain names.[91]

Proving bad faith intent to profit ensures that only genuine cases of cybersquatting are targeted by the legislation, rather than inadvertently penalizing innocent domain name registrants.[92] If the plaintiff establishes that the defendant aimed to profit from the plaintiff's trademark, then the defendant's actions are deemed intentional, not coincidental, reflecting a deliberate attempt to misuse the trademark for personal benefit.[93] Moreover, bad faith intent to profit can also help courts in determining appropriate remedies, such as damages, injunctions, or the transfer of the infringing domain name to the trademark owner.[94]

The ACPA provides nine factors to guide federal courts in determining whether a defendant has a bad faith intent to profit from a domain name.[95] These factors help establish whether the defendant's actions were intended to exploit the goodwill associated with the plaintiff's trademark.[96] These factors include:

> (1) The trademark or other intellectual property rights of the person, if any, in the domain name; (2) The extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person; (3) The person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services; (4) The person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name; (5) The person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark; (6) The person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct; (7) The person's provision of material and misleading false contact information when

---

[90] *Id.*
[91] *Id.*
[92] BOUCHOUX, *supra* note 3, at 152 exb.7-1.
[93] *Id.*
[94] *Id.*
[95] Prudential Ins. Co. of Am. v. Pru.com, 546 F. Supp. 3d 476, 484 (E.D. Va. 2021).
[96] *Id.*

> applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct; (8) The person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks; and (9) The extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous.[97]

These factors are not exhaustive, and courts may consider the totality of the circumstances when determining if a defendant's actions were intended to exploit the goodwill associated with a plaintiff's trademark.[98] For example, courts have considered the defendant's pattern of registering multiple domain names containing famous trademarks as indicative of bad faith.[99] The presence or absence of any single factor is not necessarily determinative, and courts must weigh the facts of each case to make a determination.[100]

Additionally, the ACPA includes a safe harbor provision, stating that bad faith intent shall not be found if the person believed and had reasonable grounds to believe that the use of the domain name was fair use or otherwise lawful.[101] However, courts interpret the safe harbor provision narrowly, limiting its application strictly to cases where the defendant's actions show no bad faith intent to profit.[102] For instance, defendants who act even partially in bad faith in registering a domain name are not entitled to benefit from the ACPA's safe harbor provision.[103] In *Pinehurst, Inc. v. Wick*, the court determined that the defendants did not qualify for the ACPA's safe harbor provision due to their bad faith intent to profit from the Pinehurst domain names.[104] Their actions, including attempts to "mess" with corporate America and even registering domain names after the lawsuit began, undermined any claim to such good faith.[105]

---

[97] 15 U.S.C. § 1125(d)(1)(b)(i)(I)-(IX); *see Prudential*, 546 F. Supp. 3d at 485; *see also* Wagner v. Lindawagner.com, 202 F. Supp. 3d 574 (E.D. Va. 2016).
[98] *Prudential,* 546 F. Supp. 3d at 485.
[99] Pattern[s] can be highly relevant even if it does not fit neatly into the specific factors enumerated by Congress. N. Light Tech., Inc. v. N. Lights Club, 236 F.3d 57, 65 (1st Cir. 2001).
[100] *Prudential*, 546 F. Supp. 3d at 485.
[101] S. Co. v. Dauben Inc., 324 F. App'x 309, 312 (5th Cir. 2009); *see* Interstellar Starship Servs. v. Epix, Inc., 304 F.3d 936 (9th Cir. 2002).
[102] Virtual Works, Inc. v. Volkswagen of Am., Inc., 238 F.3d 264, 270 (4th Cir. 2001).
[103] Pinehurst, Inc. v. Wick, 256 F. Supp. 2d 424, 428 (M.D.N.C. 2003) (citing *Virtual Works*, 238 F.3d at 270).
[104] *Wick*, 256 F. Supp. 2d at 430.
[105] *Id.*

While the ACPA is designed to protect legitimate domain name registrants, its narrow interpretation of the safe harbor provision can put well-intentioned registrants at risk, as even minor signs of bad faith can lead to disqualification from protection. Additionally, the subjective assessment of bad faith intent complicates legal proceedings, resulting in inconsistent judicial decisions that undermine the ACPA's goal of providing a clear and effective framework for resolving domain name disputes.

iv. The Legal Remedies

If parties dispute the rights to a domain name, the aggrieved owner has a variety of avenues in which to pursue relief. If a violation of the ACPA is established, the court may "order the forfeiture or cancellation of the [offending] domain name or [its] transfer . . . to the owner of the mark."[106] The mark owner can also seek up to three times their actual damages and obtain injunctive relief.[107] Actual damages include any profits the domain name registrant earned from using the mark, as well as losses suffered by the mark owner, like lost sales or damage to the mark's reputation.[108] On the contrary, instead of actual damages, the mark owner may choose to recover statutory damages ranging from $1,000 to $100,000 per domain.[109] The court determines the final award amount at its discretion.[110]

These remedies are not exclusive; one may pursue an action in court under the ACPA and may also initiate a proceeding under the UDRP.[111] Both the UDRP and ACPA permit recoveries for the cancellation or transfer of a domain name.[112] However, the process for the UDRP is preferred by some domain users because the policy is quick and inexpensive.[113] The UDRP is also beneficial to some domain name owners if they only wish to cancel or transfer the offending name, and not pursue monetary damages.[114] Though the ACPA may result in significant statutory damages, the disadvantage is that the court proceedings may be expensive and time-consuming for the domain name owner.[115]

---

[106] 15 U.S.C. § 1125(d)(1)(C).
[107] 15 U.S.C. § 1117(a).
[108] *Id.*
[109] 15 U.S.C § 1117(c).
[110] In "exceptional cases," attorney's fees may also be recovered. 15 U.S.C § 1117(a).
[111] BOUCHOUX, *supra* note 3, at 152; *see* Diane L. Kilpatrick, *ICANN Dispute Resolution vs. Anti-Cybersquatting Consumer Protection Act Remedies: Which Makes More "Cents" for the Client?*, 2 HOUS. BUS. & TAX L.J. 283, 291 (2001).
[112] BOUCHOUX, *supra* note 3, at 152.
[113] *Id.* at 151.
[114] *Id.*
[115] *Id.* at 151-52.

B. Fraudulent Creation of Business Entities ("FCEs")

The FCEs are actions undertaken with the intent to deceive and unlawfully profit from the misuse of another's property or rights.[116] This phenomenon often involves the establishment of business entities, such as shell companies, with the intent to deceive and profit unlawfully.[117] These activities may include evading taxes, laundering money, and defrauding creditors.[118] Similar to cybersquatters' actions, these cases revolve around two critical elements: deception and the intent to derive illicit profit from the misuse of others' assets or rights.[119]

Take, for instance, Emma Caldwell, a financial consultant, creates "Phantom Industries LLC", a shell company with no legitimate operations, to secure fraudulent business loans and evade taxes. Caldwell then fabricates the financial records to obtain high-value loans, then transfers the funds through a web of offshore accounts and fictitious vendors, laundering the money while avoiding tax liabilities. When creditors seek repayment, Phantom Industries declares bankruptcy, leaving banks and investors with millions in losses while Caldwell secretly funnels the laundered funds into personal assets hidden under different corporate names. Caldwell's scheme highlights the dangers of FCEs, demonstrating how shell companies can be exploited to deceive financial institutions, evade taxes, and manipulate bankruptcy laws.

i. An Overview of FCEs

FCEs can take various forms, both within and outside a company, often designed to deceive investors, evade taxes, or misappropriate funds.[120] An example of creating a false entity with the intent to profit can be found in the case of *Cruden Bay Holdings, LLC v. Jezierski*.[121] Defendant and his co-conspirators (collectively, "Defendants") created entities with names mimicking those of real entities to defraud potential investors.[122] The Defendants formed a new entity misleadingly named "SCUSA Financial" to make it appear as though it was associated with the legitimate entity Santander Consumer USA, which is known as "SCUSA."[123] The Defendants then opened bank accounts in the name of SCUSA Financial,

---

[116] Daniel J. Marcus, *The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information*, 68 DUKE L.J. 555, 564 (2018); *see National Small Business Week*, *supra* note 1.
[117] *See National Small Business Week, supra* note 1.
[118] *See id.*
[119] *See id.*
[120] See *id.*
[121] Cruden Bay Holdings, LLC v. Jezierski, Civil Action No. 3:21-CV-01170-E, 2022 U.S. Dist. LEXIS 25709, at *1, *6 (N.D. Tex. Feb. 14, 2022).
[122] *Id.*
[123] *Id.*

giving the illusion that funds were being sent to the legitimate SCUSA entity.[124] This fraudulent scheme was designed to deceive investors into believing that they were investing in a legitimate business, thereby the Defendants profited from the deception.[125]

Another example is found in the case of *United States v. Chun Mei Tong*, where the defendant created a false identity and a rental property entity named "Affordable Housing" operated by the fictitious identity "Debbie Kim."[126] The defendant forged the true owner's signature on an authorization form to direct payments illegally to herself.[127] This scheme was intended to profit by diverting payments from the true owner to the defendant.[128]

Additionally, in *Able Co. v. Commissioner*, the defendant created foreign business trust organizations solely for tax avoidance purposes.[129] These entities were shams with no profit objective or business purpose other than to evade federal income tax.[130] The defendant engaged in fictitious transactions between these entities, generating counterfeit contracts, promissory notes, and other documents to create the appearance of legitimate business activities, thereby profiting from the tax deductions generated by these false entities.[131]

Based on the wide scope of available deceptive practices, FCEs represent a significant threat to the integrity of financial systems, investor confidence, and regulatory frameworks. *Cruden Bay*, *Chun Mei Tong*, and *Able* exemplify the diverse tactics employed by individuals to manipulate legal structures for personal gain. Whether through misleading investors, diverting funds, or evading taxes, these schemes undermine the trust essential to legitimate business operations.[132] Regulatory measures, including legal penalties and enhanced scrutiny, play a critical role in detecting and combating such fraud.[133] Upholding corporate transparency and enforcing accountability are essential to deterring the creation of false entities and maintaining a fair, ethical marketplace.[134]

---

[124] *Id*.
[125] *Id.* at *5.
[126] United States v. Chun Mei Tong, No. 18-00082 JMS, 2023 U.S. Dist. LEXIS 169326, at *2, *7 (D. Haw. Aug. 22, 2023).
[127] *Id.* at *8.
[128] *Id.* at *12.
[129] Able Co. v. Commissioner, Docket Nos. 37272-86, 37273-86, 37274-86, 37276-86, 37277-86, 1990 Tax Ct. Memo LEXIS 553, at *6-7 (T.C. Sept. 20, 1990).
[130] *Id.* at *29.
[131] *Id.*
[132] *National Small Business Week*, *supra* note 1.
[133] *Id.*
[134] 12 U.S.C. § 5511(a).

ii. Protections Against FCEs

The regulatory landscape in the United States is designed to promote transparency, fairness, and accountability across various sectors, particularly in financial transactions, corporate governance, and consumer protection.[135] A series of federal laws and regulations, including the Major Fraud Act of 1988, Section 43(a) of the Lanham Act, Know Your Customer ("KYC") regulations, consumer protection laws, the Corporate Transparency Act ("CTA"), and doctrines like "piercing the corporate veil", collectively aim to safeguard public and governmental interests.

The Major Fraud Act directly addresses bad faith attempts to profit by criminalizing schemes to defraud the government.[136] This includes creating fraudulent business entities to secure government contracts under false pretenses, thereby unlawfully profiting from federal funds without intending to deliver genuine services.[137] Similarly, Section 43(a) of the Lanham Act combats bad faith attempts to profit through false designations of origin and false advertising, which includes the creation of businesses that falsely affiliate with established brands to deceive consumers and gain an unfair market advantage.[138]

KYC regulations, mandated primarily for financial institutions, work preemptively to deter fraud and bad faith attempts to profit.[139] To prevent fraudulent financial activity, KYC regulations require financial institutions to verify customer identities, reducing the risk of business entities being used for money laundering or tax evasion.[140] Similarly, Consumer Protection Laws and the CTA combats bad faith attempts to profit by requiring the disclosure of beneficial ownership information.[141] Further enhancing transparency, these regulations mandate the disclosure of beneficial ownership information, which helps deter the use of anonymous corporate entities for illegal activities, such as money laundering and tax fraud.[142]

Lastly, "piercing the corporate veil" regulations address bad faith attempts to profit by holding individuals accountable when they misuse

---

[135] 12 U.S.C. § 5511(b).
[136] 18 U.S.C. § 1031; s*ee* S. Rep. No. 99-345 at 1-2 (1986).
[137] *See National Small Business Week, supra note 1.*
[138] 15 U.S.C. § 1125(a); Krasnyi Oktyabr, Inc. v. Trilini Imps., 578 F. Supp. 2d 455, 470 (E.D.N.Y. 2008) (quoting N.Y. GEN. BUS. LAW § 350).
[139] Marcus, *supra* note 116, at 560; *see* Justin Brookman, *The Consumer Always Has Rights: Envisioning a Progressive Free Market: Protecting Privacy in an Era of Weakening Regulation*, 9 HAVR. L. & POL'Y REV. 355, 358-61 (2015).
[140] *See* Marcus, *supra* note 116, at 591.
[141] 12 U.S.C. § 5511(a); 32 U.S.C § 5336; *see* Brookman, *supra* note 145, at 361.
[142] *See* 12 U.S.C. § 5511(b).

corporate entities to perpetrate fraud or evade legal obligations.[143] This ensures that the corporate form cannot be misused or exploited to shield wrongful conduct.[144]

These frameworks are not exhaustive as FCEs can take various forms.[145] However, these laws specifically target fraudulent practices, deceptive advertising, financial crimes, corporate misuse, and consumer exploitation, ensuring a robust legal framework that promotes integrity.[146] Each regulation plays a distinct role in mitigating risks of misconduct while imposing stringent penalties on those who violate these rules, thereby fostering a more secure and equitable business environment.[147] Together, they provide critical ways for maintaining trust and upholding ethical standards in both public and private sectors.

iii. The Legal Standards and Elements

Establishing a false entity to profit under federal jurisdiction carries significant legal risks, including exposure to fraud claims, piercing the corporate veil for personal liability, and potential criminal liability.[148] As stated above, there are several avenues for imposing a cause of action against an FCE; each with its own set of factors and elements. However, in federal court, fraud claims must meet the stringent pleading standards of Rule 9(b), which require plaintiffs to specify the fraudulent acts with particularity, the circumstances surrounding them, and the benefit gained by the defendant.[149] These standards ensure that fraud allegations are clear enough to provide notice to the defendant and to prevent baseless claims.[150]

iv. The Legal Remedies

The standard remedies for the FCEs under federal law include setting aside fraudulent transfers, recovering property or its value, and imposing significant fines and imprisonment for criminal fraud.[151] These measures aim to restore the status quo and deter fraudulent activities.[152] The remedies for the FCEs under federal law include both civil and criminal penalties.[153] Civil remedies can involve setting aside the fraudulent transfer, recovering

---

[143] JOHN C. COFFEE JR., ET. AL., CASES AND MATERIALS ON CORPORATIONS 215 (9th ed. 2022).
[144] *Id.* at 216.
[145] *National Small Business Week*, *supra* note 1.
[146] 31 U.S.C. § 3729; 18 U.S.C. § 286.
[147] *Id.*
[148] *Id.*
[149] FED. R. CIV. P. 9.
[150] *Id.*
[151] 28 U.S.C. § 3306.
[152] *Id.*
[153] United States CFTC v. Crombie, 914 F.3d 1208, 1210 (9th Cir. 2019).

the property transferred, or obtaining a monetary judgment equivalent to the value of the property if it cannot be returned.[154]

For instance, under 11 U.S.C. § 550, a trustee may recover the property transferred or its value from the initial transferee or any subsequent transferee who took the property in bad faith or with knowledge of the voidability of the transfer.[155] In instances where a corporation adopts a name with fraudulent intent or with knowledge of an existing foreign corporation's use of that name, courts can issue injunctions to prevent the domestic corporation from continuing to use the name.[156] This legal remedy helps protect the original business from unfair competition and potential reputational damage.

FCEs can also lead to criminal penalties.[157] Federal laws impose harsh penalties for fraudulent statements or false documents in dealings with registered entities.[158] For example, under 7 U.S.C. § 13(a)(4), it is a felony punishable by a fine of up to $1,000,000 or imprisonment for up to 10 years, or both, for any person to intentionally conceal a material fact, make false or fraudulent statements, or knowingly submitting false documents to a registered entity.[159]

Under 18 U.S.C. §§ 1341 and 1343, individuals who engage in schemes to defraud using mail or wire communications can face fines up to $1,000,000 and imprisonment for up to thirty years if the fraud affects a financial institution or involves a major disaster or emergency.[160] Similarly, 18 U.S.C. § 1031 imposes penalties for defrauding the United States in connection with federal assistance or procurement, with fines up to $1,000,000 and imprisonment for up to ten years.[161] In cases involving fraudulent conveyances, courts may also consider "badges of fraud" to infer fraudulent intent, such as lack of consideration, close relationships between parties, and the timing of transactions relative to financial difficulties.[162] These factors help establish the fraudulent nature of the entity's creation and support the application of remedies.

---

[154] *Id.* at 1211.
[155] 11 U.S.C. § 550.
[156] Miami Credit Bureau, Inc. v. Credit Bureau, Inc., 276 F.2d 565, 568 (5th Cir. 1960).
[157] *Crombie*, 914 F.3d at 1212.
[158] *Id.*
[159] 7 U.S.C. § 13(a)(4); *see Crombie*, 914 F.3d at 1212.
[160] 18 U.S.C. § 1341; 18 U.S.C. § 1343.
[161] 18 U.S.C. § 1031.
[162] Badges of fraud are circumstantial evidence that courts use to infer intent in cases where there is no direct evidence of actual fraud. Langlais v. Brenner-Currier, 561 F. Supp. 3d 103, 110-11 (D.N.H. 2020).

III. ANALYSIS

A. Bad Faith Intent to Profit and Consumer Confusion

In a hypothetical scenario, imagine there is a parent company called "BrightWave Innovations, Inc." that specializes in e-commerce solutions and software development. The company has been operating for several years and has built a solid reputation, trust among clients, and significant brand recognition in the tech industry. BrightWave Innovations regularly engages in commerce, dealing with clients ranging from small businesses to large enterprises for custom software, payment gateway setups, and digital infrastructure services.

Now, suppose a second party, a former competitor or disgruntled ex-employee named Alex, takes notice of BrightWave's success and seizes an opportunity to exploit its established brand. Without the company's knowledge, Alex registers a new business under a strikingly similar name, "BrightWave Solutions, Inc.," deliberately creating confusion in the marketplace to attract and profit from BrightWave Innovations' clients. As Alex's scheme unfolds, he expands his deceptive practices by registering variations of the BrightWave domain name, escalating his actions into cybersquatting.

Both cybersquatting and FCEs are grounded in the bad faith intent to capitalize on the reputation and goodwill of an established brand, leading to confusion and consumer deception. These actions exploit legal structures, such as domain registration and business entity formation, which are intended for legitimate purposes, but are manipulated to create competitive or financial advantage by deceiving the public. While initially focused on the FCEs, Alex's broader bad faith efforts demonstrate a clear intent to profit from BrightWave Innovations. This hypothetical will help assess the application of bad faith factors, evaluate the likely outcome, and identify any remaining legal shortcomings.

To determine if Alex has a bad faith intent to profit from creating a misleading business entity, we can apply the nine ACPA factors to BrightWave Innovation's situation, drawing a parallel to domain name disputes under cybersquatting law.[163] By evaluating Alex's actions through the lens of the nine bad faith factors, it becomes apparent that these factors are equally relevant in cases of business name infringement. These factors are used to assess consumer confusion and the exploitation of brand goodwill, despite the ACPA's primary focus on domain name registration.

---

[163] There is "no clear, overarching principle that separates the fraud or bad faith claims." Harrods Ltd. v. Sixty Internet Domain Names, 302 F.3d 214, 227 (4th Cir. 2002).

Of the nine factors outlined in the ACPA, the most pertinent factors in determining bad faith intent in Alex's adoption of "BrightWave Solutions, Inc." relate to trademark rights, personal or professional connection to the name, and prior use. Under the first factor, trademark or intellectual property rights in the domain name [or business name in this case], BrightWave Innovations, Inc. likely holds strong trademark rights due to its established reputation and recognition in the tech industry, while Alex lacks such rights to the derivative name. This discrepancy underscores bad faith, as Alex's adoption of the name appears designed to mimic and exploit the goodwill of the original company. Furthermore, "BrightWave Solutions" is neither Alex's legal name nor commonly associated with him nor any prior owned business, suggesting an intent to mislead rather than a legitimate connection to the name.

Additional factors further reveal Alex's bad faith. The lack of any bona fide prior use of "BrightWave Solutions" in connection with legitimate goods or services and the absence of noncommercial or fair use purposes, such as criticism or parody, highlight the commercial intent behind the adoption of the name. The purpose appears solely to confuse clients familiar with BrightWave Innovations, attracting them under false pretenses for commercial gain. This not only undermines any claim of fair use but also threatens the goodwill and reputation of the original company by creating confusion and potential business loss.

While some factors, such as whether Alex provided false contact information or registered multiple similar names, lack specific evidence, the overarching intent to exploit BrightWave Innovations' established brand is evident. The distinctiveness and fame of the original company's name further bolster the case against Alex, as it is clear he seeks to benefit from its reputation. Even without explicit offers to sell the name or additional registrations, the intentional mimicry of BrightWave Innovations signifies bad faith and supports a conclusion of exploitative behavior.

While these nine ACPA factors are a non-exhaustive list, it is evident that Alex's registration of "BrightWave Solutions, Inc." demonstrates a bad faith intent to profit from the established brand of BrightWave Innovations.[164] Based on the application of the ACPA factors, Alex's actions are likely to cause confusion, harm the goodwill of BrightWave Innovations, and mislead consumers, thereby satisfying the criteria for bad faith intent under the ACPA and in similar cases of FCEs. Therefore, BrightWave Innovations would likely win on its ACPA claim.

Under the ACPA, BrightWave Innovations can seek several remedies against Alex for the bad faith registration of BrightWave Solutions. First,

[164] Prudential Ins. Co. of Am. v. Pru.com, 546 F. Supp. 3d 476, 482 (E.D. Va. 2021).

BrightWave Innovations could seek injunctive relief, including a court order to permanently enjoin Alex from using the infringing domain name or any substantially similar domain names, to order the transfer of the infringing domain name to BrightWave Innovations, or to order its cancellation. Second, BrightWave Innovations could pursue monetary damages, including the option to elect statutory damages ranging from $1,000 to $100,000 per domain, to seek compensatory damages, or to request the disgorgement of Alex's profits derived from the bad faith registration and use of the BrightWave name. Lastly, in "exceptional" cases, BrightWave could recover attorneys' fees and costs, with the ACPA's statutory damages provisions designed to both compensate BrightWave and deter future wrongful conduct by Alex.

Despite providing legal recourse in this situation, are these measures truly sufficient to protect BrightWave in the future? Consider the following. First, would Alex realistically be deterred from further deceptive conduct against BrightWave? While the threat of statutory damages can deter some cybersquatters, those with significant financial resources or high-profit motives may not be meaningfully discouraged by the $100,000 cap, especially if their potential gains far exceed this limit. Second, would BrightWave truly be made whole? The confusion Alex created has eroded valuable trust and goodwill that BrightWave has built over time, diverting web traffic away from its legitimate site and resulting in decreased online visibility and revenue. This situation has led to significant legal costs for reclaiming the domain name and protecting the brand. Ultimately, the brand's value has been diluted, making it more challenging for customers to find the legitimate business online and impacting overall brand integrity and market position. Without meaningful reform, businesses and consumers will continue to face the detrimental effects of cybersquatting, undermining trust and stability in the digital marketplace.

B. Modern Trends: Leading Practices and Technologies

Protections against cybersquatting and the fraudulent creation of business entities have evolved significantly to address the challenges posed by deceptive practices in the digital age. Despite these advancements, questions remain about the constitutional validity and adequacy of these laws in protecting business entities and consumers. Federal agencies have implemented several key protections to combat these issues.[165] For example, the Financial Crimes Enforcement Network ("FinCEN"), authorized by the

[165] *See National Small Business Week, supra* note 1.

USA Patriot Act of 2001, has mandated the disclosure of beneficial owners to enhance transparency.[166]

Additionally, stringent anti-money laundering regulations have been introduced to prevent illicit financial activities.[167] The Securities and Exchange Commission ("SEC") has also been active in enforcing actions to maintain the integrity of financial markets.[168] This section will first explore the impact of each business protection and its constitutional implications, followed by an examination of the effectiveness of these measures in protecting businesses and consumers. While these measures represent significant progress, continuous evaluation is essential to ensure these laws remain effective against the ever-evolving digital threats.

i. Examination of Legal Frameworks

This section provides a constitutional evaluation of key FCE legal frameworks, such as the Corporate Transparency Act ("CTA") and SEC enforcement actions, demonstrating how existing legal mechanisms attempt to address deceptive and bad faith practices. While these frameworks aim to curb fraudulent corporate activities, their effectiveness is constrained by potential constitutional conflicts, including concerns over privacy, due process, and the balance of governmental authority. This analysis underscores the broader issue that, despite current regulatory efforts, legal protections remain inadequate in fully combating cybersquatting and FCEs. By identifying these limitations, this section reinforces the necessity of expanding existing frameworks to ensure that they can more effectively prevent deceptive practices while maintaining constitutional integrity.

1. The Corporate Transparency Act & FinCEN

The CTA requires certain corporations and limited liability companies to disclose beneficial owner information to the FinCEN and update ownership information within one year of any changes.[169] As a division of the Department of the Treasury, FinCEN is responsible for developing a non-public registry tracking the beneficial owners of reporting companies, which may be shared with law enforcement and financial institutions under

---

[166] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, H.R. 3162, 117th Cong. (2001).
[167] Shawn Turner, *U.S. Anti-Money Laundering Regulations: An Economic Approach to Cyberlaundering*, 54 CASE W. RES. L. REV. 1389, 1392 (2004).
[168] Samuel J. Winer, Christopher M. Cutler & Joseph D. Edmondson, Jr., *Federal Securities Act of 1933* § 10.01 (Matthew Bender & Co. 2025); *see* SEC v. Dresser Indus., Inc., 628 F.2d 1368, 1371 (1980).
[169] 31 U.S.C. § 5336.

certain circumstances.[170] The stated purpose of these requirements is to combat money laundering, terrorist financing, corruption, tax fraud, and other illicit activities while imposing a minimum burden on entities doing business in the United States.[171]

Since its adoption, however, the CTA has raised several significant issues regarding its mandatory disclosure requirements, including constitutional concerns, legal challenges, and potential burdens on businesses and organizations. These issues have sparked debates over the limits of congressional authority, the scope of federal regulatory power, and the balance between transparency and administrative feasibility.

a. Constitutional Concerns

The primary constitutional issues surrounding the CTA revolve around the scope of Congress' legislative powers. In the recent case of *Nat'l Small Bus. United ("NSBA") v. Yellen*, a group of plaintiffs, including approximately sixty-five thousand businesses and entrepreneurs, filed a lawsuit against the U.S. Department of the Treasury.[172] The plaintiffs argued that the CTA exceeded Congress' authority under Article I of the U.S. Constitution.[173] Specifically, they claimed that the CTA's mandatory beneficial ownership disclosure requirements exceeded Congress' powers to regulate interstate commerce, oversee foreign affairs and national security, and impose taxes.[174]

The district court ruled in favor of the plaintiffs and found that the CTA was unconstitutional on each of these grounds.[175] The ruling emphasized that the CTA failed to regulate the channels and instrumentalities of commerce, meaning it did not directly govern commercial transactions or economic activity across state lines.[176] Furthermore, the court determined that the civil penalties for noncompliance did not constitute a tax and, therefore, could not be justified under Congress' taxing power.[177]

---

[170] Fin. Crimes Enf't Network, FIN-220-A003, *Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)*, at 1-2 (2020), [https://perma.cc/5ACQ-2C78].
[171] *Id.* at 8.
[172] Nat'l Small Bus. United v. Yellen, 721 F. Supp. 3d 1260, 1267 (N.D. Ala. 2024).
[173] Article I of the U.S. Constitution grants Congress several legislative powers, including the power to lay and collect taxes, regulate commerce with foreign nations and among the states, and make all laws necessary and proper for executing its powers. *Id.*; *see* U.S. CONST. art. I.
[174] *Yellen*, 721 F. Supp. 3d at 1267, 1280.
[175] *Id.* at 1289.
[176] *Id.* at 1280.
[177] *Id.* at 1288.

NSBA is currently on appeal to the Eleventh Circuit, and further developments may affect the legal landscape going forward.[178] However, the court suggested that a narrower version of the CTA could withstand constitutional scrutiny if it were explicitly limited to entities engaged in interstate commerce or directly tied to tax collection purposes.[179] This ruling signals potential pathways for legislative modifications that could strengthen the CTA's constitutional foundation while still achieving its transparency goals.

The CTA also raises additional concerns regarding privacy protections under the Fourth Amendment. Some criticize that the CTA violates the Fourth Amendment by its mandatory disclosure provisions. The Fourth Amendment protects individuals and entities against unreasonable searches and seizures by the federal government.[180] This protection extends to administrative proceedings, including those conducted by the Federal Trade Commission.[181]

Nevertheless, the FinCEN's requirement for corporations to disclose beneficial ownership information could be seen as a form of government search under the Fourth Amendment, potentially violating privacy rights.[182] These disclosure provisions mandate that private entities disclose sensitive personal information to federal law enforcement, even if these entities are not involved in criminal activities or engaged in interstate or foreign commerce.[183] Although the court in *Yellen* has not yet resolved this issue, the claims presented in the case indicate the likelihood of continued legal challenges across various jurisdictions, underscoring the need for further examination of these privacy concerns.[184]

---

[178] Freeny, Kyle R., et al., *District Court Declares Corporate Transparency Act Unconstitutional*, 15 NAT'L L. REV. 52, (Mar. 7, 2024), https://natlawreview.com/article/district-court-declares-corporate-transparency-act-unconstitutional.

[179] *Yellen*, 721 F. Supp. 3d at 1288-89.

[180] U.S. CONST. amend. IV.

[181] *Id.*; *see* FTC v. Pointbreak Media, LLC, 343 F. Supp. 3d 1282, 1296-97 (S.D. Fla. 2018).

[182] *Yellen*, 721 F. Supp. 3d at 1267.

[183] 31 U.S.C. § 5336.

[184] *Yellen*, 721 F. Supp. 3d at 1289. The plaintiff's suit is not the first to challenge the law, as parties in multiple jurisdictions have sued to enjoin the enforcement of the CTA and its reporting rule, with courts reaching differing conclusions about the law's constitutionality. *See* Smith v. United States Dep't of the Treasury, No. 6:24-cv-336-JDK, 2025 U.S. Dist. LEXIS 2321, at *2 (E.D. Tex. Jan. 7, 2025) ("The plaintiff's suit is not the first to challenge the law, as parties in multiple jurisdictions have sued to enjoin the enforcement of the CTA and its reporting rule, with courts reaching differing conclusions about the law's constitutionality."); *see also* Texas Top Cop Shop, Inc. v. Garland, 2024 U.S. Dist. LEXIS 218294 (E.D. Tex. Dec. 5, 2024) (finding the CTA is likely unconstitutional); *Yellen*, 721 F. Supp. 3d at 1260 (finding the CTA is unconstitutional and granting a permanent injunction); Firestone v. Yellen, 2024 U.S. Dist. LEXIS 170085 (D. Or. Sept. 20, 2024) (finding the CTA is likely constitutional).

b. The Broader Legal Landscape: Challenges and Burdens on Organizations.

The CTA has also faced significant legal challenges that have hindered its implementation, largely due to concerns from business organizations and advocacy groups who argue that it imposes undue burdens on small businesses and nonprofits.[185] These groups have raised significant concerns that the CTA's complex reporting requirements create significant compliance and administrative challenges, particularly for smaller organizations that lack the robust legal and financial infrastructure of larger corporations.[186] Many of these entities operate with limited resources and volunteer-based support, leaving them ill-equipped to meet the CTA's stringent federal mandates.[187] As a result, they face a disproportionate regulatory burden that may hinder their operations and divert critical resources away from their core missions.

Critics further assert that the CTA disproportionately impacts these entities and encroaches upon states' traditional authority over corporate formations.[188] Both of these concerns are compounded by the severe penalties for noncompliance, including substantial fines and imprisonment, which may be imposed even in cases where violations occur beyond the control or awareness of the business.[189] Taken together, these objections underscore the view that the CTA, though aimed at enhancing transparency, may inadvertently penalize the very organizations least able to absorb its demands.

In response, a notable development occurred in December 2024 when a federal judge in Texas issued a nationwide preliminary injunction blocking the CTA's reporting requirements.[190] The judge found that the CTA exceeds Congress's power and intrudes on states' traditional authority over matters of corporate formation, violating the federalism principle that separates state and federal powers.[191] The injunction came just weeks before the compliance deadline, leading to significant confusion and disruption. The government promptly appealed against the injunction, and the Fifth Circuit issued conflicting orders, ultimately leading to the Supreme Court granting

---

[185] *Yellen*, 721 F. Supp. 3d at 1267.
[186] Northport Health Servs. of Ark., LLC v. United States HHS, 14 F.4th 856, 876 (8th Cir. 2021).
[187] *Id.*
[188] *Id.* at 877.
[189] *Smith*, No. 6:24-cv-336-JDK, U.S. Dist. LEXIS 2321, at *17.
[190] Tex. Top Cop Shop, Inc. v. Garland, Civil Action No. 4:24-CV-478, 2024 U.S. Dist. LEXIS 218294, at *116 (E.D. Tex. Dec. 3, 2024).
[191] *Id.* at *68.

a stay of the nationwide injunction.[192] This series of legal maneuvers has created uncertainty for businesses and legal practitioners regarding the enforcement of the CTA's reporting requirements.

The impact of these legal challenges to the CTA underscores the tension between federal transparency efforts and the autonomy of state-level business regulations. While this Note does not examine the substance of these challenges, it acknowledges the significant confusion and disruption they have caused for business owners, who face uncertainty regarding compliance requirements and potential penalties. The ongoing litigation and appeals will continue to shape the future effectiveness, enforcement, and implementation of the CTA.

Overall, the CTA's mandatory disclosures have sparked a complex debate involving constitutional authority, legal challenges, and the practical impact on businesses and organizations. While the law aims to enhance corporate transparency and prevent illicit financial activities, its implementation has revealed significant legal and administrative hurdles. Moving forward, policymakers will need to consider legislative adjustments to address constitutional concerns, refine enforcement mechanisms, and reduce compliance burdens to ensure that transparency efforts do not unduly hinder legitimate business operations.

2. Security and Exchange Commission ("SEC") Enforcement Actions

The SEC enforcement actions bring up constitutional concerns around the Seventh Amendment's right to a jury trial, the Appointments Clause of Article II, and The Nondelegation Doctrine. These constitutional issues arise from the SEC's procedures for adjudicating enforcement actions and the appointment and removal of its administrative law judges ("ALJs").[193] As the SEC increasingly relies on its own ALJs for adjudication, these issues have garnered significant legal scrutiny regarding the separation of powers and fairness in administrative proceedings.

a. The Seventh Amendment's Right to a Jury Trial

A more sweeping Supreme Court decision was recently delivered in *SEC v. Jarkesy*, which affirmed a Fifth Circuit ruling that found the SEC'S ALJ process to violate a defendant's Seventh Amendment right to a jury trial. In *Jarkesy*, the SEC accused Jarkesy and his advisory firm, Patriot28,

---

[192] William E. Quick, et al., *UPDATE: Government Appeals Corporate Transparency Act Injunction to the U.S. Supreme Court*, 15 NAT'L L. REV. 57, (Jan. 2, 2025), https://natlawreview.com/article/update-government-appeals-corporate-transparency-act-injunction-us-supreme-court.

[193] Jarkesy v. SEC, 34 F.4th 446, 450 (5th Cir. 2022).

of defrauding investors in two hedge funds by misrepresenting key information and overvaluing assets to inflate fees.[194] The SEC's ALJs found them liable, and the Commission upheld the decision.[195] Jarkesy appealed, challenging the constitutionality of the SEC's administrative proceedings.[196]

The Fifth Circuit Court of Appeals ruled in Jarkesy's favor on three constitutional grounds.[197] First, it held that the SEC violated Jarkesy's Seventh Amendment right to a jury trial because the enforcement action sought civil penalties common of traditional legal claims, and securities fraud is not a "public right" that can be exclusively adjudicated by an administrative agency.[198] Second, the court found that Congress had improperly delegated legislative power to the SEC by allowing it to choose between federal courts or internal proceedings without providing an intelligible principle to guide that discretion, violating Article I via the long inert nondelegation doctrine.[199] Third, the court ruled that the removal protections for SEC ALJs, which include multiple layers of for-cause removal, violated the Article II Take Care Clause by limiting the President's ability to oversee executive functions.[200]

The Supreme Court affirmed the Fifth Circuit's rulings and issued a broader decision, striking down the SEC's ALJ process as unconstitutional under the Seventh Amendment, while leaving the other two constitutional questions unresolved.[201] The Court dismissed the SEC's claims that these actions created "new statutory obligations" under the "public rights" exception to the Seventh Amendment, rejecting previous interpretations that classified securities fraud as a "public right" suitable for administrative adjudication.[202] The Court determined that SEC actions seeking civil penalties for securities fraud are "legal in nature" and involve "a type of remedy at common law that could only be enforced in courts of law," thus protecting them under the Seventh Amendment's jury trial requirement.[203]

With the Supreme Court's resolution of the issue and removal of the SEC's discretion to bring civil penalty claims before ALJs, the SEC must now fundamentally reconsider its litigation and enforcement strategies. Even before the Supreme Court's ruling, the Fifth Circuit's decision had

---

[194] *Id.*
[195] *Id.*
[196] *Id.*
[197] *Id.* at 465.
[198] The Seventh Amendment does not mandate a jury trial for administrative proceedings involving "public rights." *Id.* at 457; *See* U.S. CONST. amend. VII.
[199] *Jarkesy*, 34 F.4th at 450.
[200] *Id.* at 465.
[201] SEC v. Jarkesy, 603 U.S. 109, 140-41 (2024).
[202] *Id.* at 137.
[203] *Id.* at 125.

already cast serious doubt on the future of the SEC's ALJ courts and those of other federal agencies. Ultimately, this decision underscores significant constitutional questions surrounding administrative adjudication, which are likely to be revisited in future cases.

b. The Appointments Clause of Article II

The SEC's administrative proceedings have also been criticized as violating the Appointment's Clause. This criticism stems from the agency's consolidation of prosecutorial, adjudicative, and appellate functions, raising constitutional issues related to procedural fairness, the separation of powers, and the legitimacy of delegated enforcement authority. The Appointments Clause, found in Article II, Section 2, Clause 2 of the U.S. Constitution, sets forth the methods for appointing federal officers.[204] It ensures that only those appointed in accordance with constitutional procedures can exercise federal power, preserving the legitimacy of administrative actions and guarding against overreach.

As regulatory efforts expand to address growing digital threats, like cybersquatting and FCEs, constitutional safeguards, such as the Appointments Clause, are becoming increasingly important to ensure lawful enforcement. Ignoring these safeguards reduces the validity of enforcement actions, exposing them to invalidation on structural grounds regardless of the intent behind them. The constitutional validity of agency enforcement does not end with the SEC; it implicates a broader array of decision-makers across trademark and internet fraud enforcement. Administrative judges at the U.S. Patent and Trademark Office, officials within the Federal Trade Commission or Department of Justice, and UDRP panelists may likewise hold appointments that fall short of constitutional requirements. This raises serious legal questions about the legitimacy of their authority and the long-term enforceability of their decisions.

The Supreme Court considered this issue in *Lucia v. SEC*, where Lucia, a financial advisor, was charged by the SEC for fraudulent marketing practices related to his "Buckets of Money" retirement strategy.[205] An SEC-appointed ALJ, Cameron Elliot, found Lucia guilty and imposed sanctions. On appeal, Lucia contended that the ALJ was unconstitutionally appointed, as the Appointments Clause requires ALJs to be appointed by the President or a department head, not SEC staff.[206] Both the SEC and the D.C. Circuit

[204] The Appointments Clause states that only the President, with the advice and consent of the Senate, can appoint principal officers, while Congress may authorize the President alone, a court of law, or a head of department to appoint inferior officers. U.S. CONST. art. II, § 2, cl. 2.
[205] Lucia v. SEC, 585 U.S. 237, 242 (2018).
[206] *Id.* at 243.

Court rejected Lucia's argument, deeming SEC ALJs as employees, not officers.[207]

However, the Supreme Court reversed and held that SEC ALJs are officers of the United States and must be appointed by the President, a court of law, or a head of department.[208] This requirement is based on the significant discretion and important functions exercised by SEC ALJs because they hold continuing offices established by law and exercise significant authority in their roles, such as taking testimony, ruling on evidence, and issuing decisions with independent effect.[209] The Court emphasized that the Appointments Clause prescribes the exclusive means of appointing officers.[210] Therefore, the SEC's practice of having staff members appoint ALJs did not comply with this constitutional requirement.[211] The impact of this case extends to broader implications for the appointment processes of federal officials and highlights the constitutional requirements for appointing officers.

The issue resurfaced in *Jarkesy*, where the Appointments Clause was again used to challenge the constitutionality of SEC ALJs appointments. Although the Supreme Court chose not to address the issue, the Fifth Circuit determined that SEC ALJs are "inferior officers" under the Appointments Clause, as established in *Lucia*, and must be appointed accordingly.[212] The court further held that, as inferior officers, SEC ALJs hold significant roles in executing the laws, which necessitates presidential control over their functions to ensure the faithful execution of laws under the Take Care Clause of Article II.[213] The court found that the statutory removal protections for SEC ALJs violated the Appointments Clause and the Take Care Clause by excessively insulating the ALJs from presidential control.[214]

Together, *Lucia* and *Jarkesy* reaffirm the constitutional boundaries on the SEC's executive authority, emphasizing the need for strict compliance with the Appointments Clause to preserve the proper separation of powers. Nonetheless, the SEC maintains that its administrative proceedings are constitutional, asserting that ALJs do not qualify as "inferior officers" and are therefore exempt from the Appointments Clause.[215] These developments

---

[207] *Id.*
[208] *Id.* at 252; *see* Joseph Forrester Trucking v. Dir., OWCP, 987 F.3d 581, 584 (6th Cir. 2021).
[209] Ramsey v. Comm'r of Soc. Sec., 973 F.3d 537, 547 (6th Cir. 2020) (quoting *Lucia,* 585 U.S. at 248).
[210] Cottonham v. Kijakazi, No. CIV-21-1013-P, 2022 U.S. Dist. LEXIS 100410, at *13 (W.D. Okla. June 6, 2022) (quoting *Lucia,* 585 U.S. at 244).
[211] *Lucia*, 585 U.S. at 245.
[212] *See Jarkesy*, 34 F.4th at 450, 463-64.
[213] *Id.*
[214] *Id.* at 465.
[215] *Id.* at 464.

illustrate that unresolved questions about administrative legitimacy are likely to persist as agencies confront novel enforcement challenges in the digital age.

c. The Nondelegation Doctrine

Lastly, constitutional challenges rooted in the Nondelegation Doctrine introduce ambiguity into the scope of agency authority, ultimately undermining the effectiveness and legitimacy of administrative governance. When agencies like the SEC or FinCEN are limited, or second guessed in their enforcement discretion, it becomes harder to pursue and deter bad faith actors involved in cybersquatting or FCEs.

The Nondelegation Doctrine allows Congress to delegate legislative power if it provides an intelligible principle to guide the exercise of the delegated authority.[216] The Supreme Court has upheld Congress's ability to delegate power under broad standards, and current doctrine does not find such delegations unconstitutional.[217] While the Court requires only an intelligible principle to guide an agency's exercise of delegated authority, the doctrine still invites legal scrutiny. For instance, the Fifth Circuit in *Jarkesy* questioned the SEC's discretion to choose whether to bring enforcement actions internally or in federal court, arguing that such discretion violates the Nondelegation Doctrine because it lacks an intelligible principle to guide it.[218] These ongoing constitutional challenges create uncertainty that weakens agencies' ability to act decisively and crack down on cybersquatting and fraudulent entities.

As mentioned above, the Fifth Circuit found that Congress had improperly delegated legislative power to the SEC by allowing it to choose between federal courts or internal proceedings without providing an intelligible principle to guide that discretion, violating Article I via the long inert Nondelegation Doctrine.[219] While the Supreme Court declined to resolve this issue, it raises concerns about whether Congress has provided adequate guidance to the SEC in making such decisions, which is a core aspect of the Nondelegation Doctrine.

Additionally, the Nondelegation Doctrine is closely related to the Major Questions Doctrine, which requires that significant policy decisions be made by Congress rather than delegated to agencies.[220] This doctrine

---

[216] United States v. Berberena, 694 F.3d 514, 523 (3d Cir. 2012).
[217] United States v. Brown, 348 F.3d 1200, 1216 (10th Cir. 2003) (quoting Touby v. United States, 500 U.S. 160, 165 (1991)).
[218] *Jarkesy*, 34 F.4th at 461-62.
[219] *See id.* at 463-65.
[220] *See* CONG. RSCH. SERV., IF12077, *The Major Questions Doctrine*, 1-2 (2022), https://crsreports.congress.gov/product/pdf/IF/IF12077 (explaining the Major Questions Doctrine requires that Congress speak clearly if it wishes to delegate decisions of vast economic and political significance to an agency).

ensures that any major regulatory actions by agencies, like the SEC, must be clearly authorized by Congress, thereby maintaining democratic accountability and preventing overreach by unelected officials.[221]

This principle has been applied in various contexts to limit the scope of agency authority and ensure that significant regulatory decisions are made through the legislative process. For instance, in *West Virginia v. EPA*, the Supreme Court underscored that the EPA's authority to regulate emissions under the Clean Air Act did not extend to implementing a generation-shifting scheme with substantial economic and political impacts without clear congressional authorization.[222] The Court found that such a significant decision required explicit delegation from Congress, rather than being inferred from broad statutory language.[223]

The principles from both *Jarkesy* and *West Virginia v. EPA* highlight significant constitutional concerns surrounding administrative adjudication, particularly regarding the limits of agency power. Both cases emphasize that major regulatory decisions must be made through the legislative process, not by administrative agencies, reinforcing the Nondelegation Doctrine. Likewise, these constitutional issues are likely to be revisited in future cases, raising further questions about the boundaries of agency authority and the role of Congress in guiding administrative actions.

With courts narrowing agency discretion through doctrines like Nondelegation, Congress can no longer afford to remain passive. It must take decisive action by drafting laws that clearly and explicitly authorize regulatory efforts. The existing legal frameworks are inadequate because they lack the precision and flexibility necessary to address the complexities of an evolving regulatory landscape. Without legislative expansion and clarification, agencies will lack the authority they need to effectively combat deceptive practices and protect the public interest.

In light of this, the growing prevalence of deceptive practices, such as cybersquatting and FCEs, reflects not the absence of enforcement tools, but the diminished efficacy of those tools due to persistent legal and constitutional uncertainty. Challenges to the enforcement of the CTA, FinCEN regulations, and actions undertaken by the SEC have generated considerable confusion and inconsistency within the regulatory landscape.[224] This uncertainty has weakened deterrence, stalled

---

[221] *Id.*
[222] West Virginia v. EPA, 597 U.S. 697, 735 (2022).
[223] *Id.* at 722-23.
[224] *See* Madeline Hughes, et al., *U.S. Supreme Court Restrictions on Regulatory Agencies Will Invite Legal Challenges*, MLEX (June 28, 2024), https://mlex.shorthandstories.com/us-supreme-court-restrictions-on-regulatory-agencies-will-invite-legal-challenges/index.html; Coinbase, Inc. v. SEC, 126 F.4th 175, 214 (3d Cir. 2025) (Bibas, J., concurring).

enforcement efforts, and compromised the capacity of institutions to prevent fraudulent behavior.[225] As a result, deceptive practices have flourished, enabling bad actors to exploit regulatory gaps with minimal consequences, to the detriment of both consumers and legitimate businesses.[226] In response, it is critical for policymakers to resolve these legal uncertainties, reinforce enforcement authority, and ensure that transparency measures support regulatory goals without imposing undue burdens on compliant businesses.

ii. Other Limitations on Protections for Consumers and Business Owners

In 2023, the World Intellectual Property Organization ("WIPO") experienced a record year in domain name dispute filings, handling nearly 6,200 complaints under its UDRP.[227] This represented a significant rise of more than 7% from 2022 and a remarkable 68% increase since the onset of the COVID-19 pandemic in 2020.[228] Looking backwards, the ACPA, enacted in 1999, was well-suited for addressing the cybersquatting issues prevalent at that time. However, the evolution of cybersquatting tactics demands updates to the law to account for new technologies and strategies.

1. The ACPA Shortcomings

Despite its utility in combating cybersquatting, the ACPA faces significant limitations that undermine its enforcement and overall effectiveness.[229] Key challenges, such as jurisdictional issues, the challenge of proving bad faith, and the rapid pace of technological advancements, highlight the inadequacy of the ACPA in offering a comprehensive solution.[230] To effectively combat these challenges, it is crucial to expand and adapt the ACPA's framework, ensuring that legal protections evolve alongside the ever-changing landscape of digital commerce and fraud.

One of the primary weaknesses of the ACPA is its limited effectiveness against international cybersquatters.[231] The statute allows for in rem jurisdiction over domain names, which can be useful when the defendant is difficult to locate.[232] This provision enables trademark owners to bring claims directly against the domain name itself, bypassing the need to

[225] *See, e.g.,* SEC v. Manor Nursing Ctrs., Inc., 458 F.2d 1082, 1104 (2d Cir. 1972).
[226] *See National Small Business Week, supra* note 1.
[227] *Record Number of Domain Name Cases filed with WIPO in 2023*, WORLD INTELL. PROP. ORG., https://www.wipo.int/amc/en/domains/caseload.html (last visited Oct. 04, 2024).
[228] *Id.*
[229] Magier, *supra* note 8, at 417, 420-21.
[230] *Id.* at 420-21.
[231] *See id.* at 417, 448.
[232] *Id.* at 417, 423.

establish personal jurisdiction over the foreign defendant.[233] However, enforcing judgments against foreign actors remains challenging, as international legal cooperation and enforcement mechanisms are often limited.[234]

Second, proving bad faith under the ACPA can be difficult, especially when cybersquatters employ sophisticated tactics to mask their intentions.[235] The statute includes a safe harbor provision that protects those who believed and had reasonable grounds to believe that their use of the domain name was lawful.[236] This provision can complicate efforts to prove bad faith, as defendants may present legitimate-sounding reasons for their actions.[237]

Additionally, courts are not restricted to the nine enumerated factors in determining bad faith intent to profit. Instead, they may consider the totality of the circumstances, as recognized in *Newport News Holdings Corp. v. Virtual City Vision*.[238] In this case, the court used a totality of circumstances approach to assess bad faith intent to profit under the ACPA, emphasizing that it was not limited to the nine factors outlined in the Act.[239] The court considered various aspects of the case, such as the defendants' delay in filing a recusal motion and their shift in website content from city information to women's fashion, which created a likelihood of confusion with the plaintiff's mark.[240] While this flexibility allows courts to address unique case-specific circumstances, it also creates challenges in establishing a consistent standard for bad faith, leading to judicial inconsistency.[241]

Lastly, when considering modern technological advancements, the ACPA was enacted at a time when cybersquatters manually registered individual domain names.[242] Today, technological advancements, such as AI tools, allow for the automatic generation of thousands of domain names

---

[233] *Id.* at 423.
[234] *Id.* at 436.
[235] Prudential Ins. Co. of Am. v. Pru.com, 546 F. Supp. 3d 476, 482 (E.D. Va. 2021) (explaining there is no one-size fits all method when assessing bad faith by a domain holder, and accordingly, nine factors are provided for consideration).
[236] S. Co. v. Dauben Inc., 324 F. App'x 309, 312 (5th Cir. 2009).
[237] See *id.* at 316-17.
[238] Newport News Holdings Corp. v. Virtual City Vision, 650 F.3d 423, 435 (4th Cir. 2011).
[239] *Id.* at 435-36
[240] *Id.* at 438.
[241] Defining the limits of "bad faith intent to profit" has been difficult because the ACPA expressly allows consideration of factors beyond those listed in the statute … an overview of the statute's purpose and the doctrine designed to implement it reveals the potential difficulties of applying traditional bad faith analysis to a case like this one. *See* Gioconda Law Grp. PLLC v. Kenzie, 941 F. Supp. 2d 424, 430-33 (S.D.N.Y. 2012).
[242] Daniel Hancock, *You Can Have It, but Can You Hold It?: Treating Domain Names as Tangible Property*, 99 KY. L.J. 185, 207 (2010).

with slight variations.[243] This overwhelms the ability of trademark owners to detect and respond to all potential infringements. While the ACPA provides retroactive application and remedies such as forfeiture, cancellation, or transfer of domain names, it does not address the scale and speed at which modern cybersquatting can occur.[244] The statute's limitations on damages for domain names registered before its enactment further reduce its deterrent effect.[245]

2. The UDRP Shortcomings

Likewise, the UDRP has been a key mechanism for resolving domain name disputes, but also faces several limitations in effectively combating cybersquatting.[246] For instance, its narrow range of remedies, the increasing sophistication of cybersquatters, and the difficulties of enforcing decisions across borders undermine the UDRP's overall impact.[247] As cybersquatting tactics evolve and become more complex, these weaknesses reveal the need for enhanced measures or reforms to bolster the UDRP's ability to deter bad faith actors and ensure more consistent enforcement across different jurisdictions.[248]

First, one of the key limitations in the UDRP's ability to fully combat cybersquatting is the narrow range of available remedies the UDRP offers.[249] Unlike traditional court proceedings, the UDRP does not provide emergency relief or monetary damages, which can be crucial for trademark owners seeking comprehensive legal solutions.[250] Instead, UDRP remedies are limited to domain cancellation or transfer, which may not sufficiently deter cybersquatters or compensate for brand harm.[251]

Another limitation is the UDRP's narrow focus on "abusive" or "bad faith" registration, which restricts its scope to only certain types of cybersquatting cases.[252] This narrow approach means that the UDRP cannot address cases involving nuanced or borderline instances of trademark

---

[243] Projects using generative technologies, including both algorithmic generation and generative artificial intelligence (AI), might have concerns over whether they can protect their artwork under U.S. copyright law. Christa J. Laser, *Legal Issues in Blockchain, Cryptocurrency, and Non-Fungible Tokens (NFTs)*, 102 NEB. L. REV. 761, 799 (2024).
[244] Kilpatrick, *supra* note 111, at 317.
[245] 15 U.S.C § 1117.
[246] Kilpatrick, *supra* note 111, at 324.
[247] *See generally id*. (describing that while the UDRP and ACPA cover one another's deficiencies, the UDRP cannot alone account for advances in cybersquatting provided its limited remedies).
[248] *Id.*
[249] BOUCHOUX, *supra* note 3, at 151-53; Kilpatrick, *supra* note 111, at 324.
[250] *Id.*
[251] *Id.*
[252] Cerruti 1881 s.a.s. v. Gurpreet Johar, WIPO Case No. D2012-1574 (WIPO Arb. & Med. Center 2012).

infringement in domain names, limiting its effectiveness against sophisticated forms of cybersquatting.[253] As cybersquatters have become more sophisticated and new generic top-level domains ("gTLDs") have emerged, cybersquatting opportunities have multiplied.[254] These new gTLDs denote the intended function of that portion of the domain space and allow for more customized and specific domain extensions, such as ".tech", ".store", ".app", or even ".brand-specific" extensions (e.g., ".google" or ".amazon"), providing more options for businesses and individuals to register unique domain names.

In the mid-1980s, the Internet Engineering Task Force introduced the first six gTLDs through RFC 920, including ".com" for commercial sites, ".org" for non-profits, ".net" for network technologies, and ".edu" for educational institutions, among others.[255] Since then, the number of gTLDs has surged to nearly 1,600, with ICANN continuously releasing new gTLDs into the marketplace.[256] For instance, ".biz", ".info", ".store", and ".tech", reflecting the ongoing demand for new domains.[257] This proliferation of gTLDs has enabled cybersquatters to exploit gaps in the UDRP, making it harder for brand owners to curb abusive domain registrations.[258]

Lastly, enforcing UDRP decisions across borders presents a major challenge, as the policy does not prevent domain registrants or complainants from pursuing court actions either before or after UDRP proceedings.[259] Jurisdictional issues can arise when a cybersquatter, for example, challenges the outcome of a UDRP arbitration in another country's court, as in cases involving U.S. courts and foreign trademark owners.[260] This is especially problematic when a prevailing foreign trademark owner under the UDRP lacks commercial use of their mark in the U.S., making it difficult to enforce favorable UDRP outcomes domestically.[261]

Ultimately, while the ACPA's and UDRP's legal frameworks attempt to address basic forms of cybersquatting, they continue to face significant limitations that undermine their effectiveness in combating modern deceptive and bad faith practices. The ACPA's jurisdictional limitations, the challenge of proving bad faith, and the rapid pace of technological

---

[253] *See id.*
[254] *See* Ashlie Smith, *Trademark Holders Beware: Source-Indicating Gtlds Are Here*, 57 IDEA 153 (2017) (explaining that new gTLDs refer to the expanded set of domain extensions introduced after ICANN broadened the domain name system beyond traditional gTLDs like ".com", ".org", and ".net").
[255] *Id.*
[256] *Id.* at 155.
[257] *See id.* at 156.
[258] *Id.*
[259] Holger P. Hestermeyer, *The Invalidity of ICANN's UDRP Under National Law*, 3 MINN. INTELL. PROP. REV. 1, 30 (2002).
[260] *Id.* at 30-31.
[261] *Id.* at 31.

advancements hinder its effectiveness. Similarly, the UDRP's narrow range of remedies and difficulties in enforcing decisions across borders limit its impact.

Since 1999, technology has experienced significant advancements, growing more sophisticated and complex, which has resulted in substantial changes to the digital landscape and the manner in which business operations and communications are conducted. As modern cybersquatting tactics have evolved, it has become increasingly difficult for existing legal frameworks to effectively address these practices, leading to a progressive decline in their success at deterring such conduct. Given these limitations, it is imperative to expand and adapt the ACPA and UDRP to address the growing complexities of the rapidly evolving digital commerce landscape. This expansion should not only broaden the jurisdiction and remedies available but also enhance international cooperation to ensure more effective enforcement of decisions and better protection for trademark owners.

IV. CONCLUSION

The expansion of deceptive practices in domain name registration and business entity creation demonstrates the inadequacy of current legal protections in addressing bad faith exploitation. Emerging technologies like AI-generated domain names have only intensified these challenges and enabled cybersquatters to evade existing regulations and target businesses with increasing sophistication. These deceptive practices are not on the rise by chance, but because enforcement has failed to keep pace. While the ACPA, the UDRP, and similar FCE legislation provide a foundational framework, their limitations continue to leave business owners vulnerable to financial harm and reputational damage. These current statutory provisions often fail to prevent bad faith actors from exploiting the system, necessitating comprehensive legislative reform.

ACPA reform should prioritize strengthening the bad faith requirement to target cybersquatters more precisely and deter malicious registrations. In addition, addressing the proliferation of AI-generated domain names and imposing monetary penalties for bulk registrations can help mitigate large-scale, automated cybersquatting operations. Furthermore, expanding the ACPA's jurisdiction through clear extraterritorial provisions and facilitating cross-border collaboration will likewise enhance its effectiveness in an increasingly interconnected global marketplace.

Reforming the UDRP is equally critical to strengthening international enforcement of domain name disputes. For instance, expanding global enforcement mechanisms and fostering mutual recognition of judgments across jurisdictions will streamline dispute resolution and ensure more

consistent outcomes. Enhanced international cooperation is necessary to close jurisdictional gaps and limit the ability of cybersquatters to exploit differences in national legal frameworks.

The same can be said for FCE legislation. FinCEN, the CTA, and SEC enforcement actions are essential for combating fraudulent business crimes, but require reform to address existing gaps. Similar to the ACPA, reform efforts should focus on narrowing the CTA's scope, enhancing FinCEN's capabilities and frameworks, and ensuring consistent, robust SEC enforcement to improve transparency, accountability, and market integrity.

Ultimately, these reforms will offer stronger protections for business owners, ensure greater consistency in domain name dispute resolution, and uphold the integrity of the digital marketplace in an era of rapid technological advancement. To that end, policymakers have a pivotal opportunity to restore clarity, reinforce enforcement, and ensure that efforts to increase transparency do not come at the expense of legitimate, good-faith businesses.