ARBITRATION
AND
MEDIATION CENTER

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

ADMINISTRATIVE PANEL DECISION
Equifax Inc. v. Patrick Sayler
Case No. D2023-0283

1. The Parties

Complainant is Equifax Inc., United States of America ("United States"), represented by The GigaLaw Firm, Douglas M. Isenberg, Attorney at Law, LLC, United States.

Respondent is Patrick Sayler, United States, represented by Wardlow Law, LLC, United States.

2. The Domain Name and Registrar

The disputed domain name <equifaxsecurity.com> (hereinafter the "Disputed Domain Name") is registered with NameCheap, Inc. (the "Registrar").

3. Procedural History

The Complaint was filed with the WIPO Arbitration and Mediation Center (the "Center") on January 21, 2023. On January 23, 2023, the Center transmitted by email to the Registrar a request for registrar verification in connection with the Disputed Domain Name. On the same day, the Registrar transmitted by email to the Center its verification response disclosing registrant and contact information for the Disputed Domain Name, which differed from the named Respondent (Redacted for Privacy / Privacy service provided by Withheld for Privacy ehf) and contact information in the Complaint. The Center sent an email communication to Complainant on January 24, 2023, providing the registrant and contact information disclosed by the Registrar, and inviting Complainant to submit an amendment to the Complaint. An informal communication email was received from Respondent on January 24, 2023. Complainant filed an amendment to the Complaint on January 25, 2023.

The Center verified that the Complaint together with the amendment to the Complaint satisfied the formal requirements of the Uniform Domain Name Dispute Resolution Policy (the "Policy" or "UDRP"), the Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules"), and the WIPO Supplemental Rules for Uniform Domain Name Dispute Resolution Policy (the "Supplemental Rules").

In accordance with the Rules, paragraphs 2 and 4, the Center formally notified Respondent of the Complaint, and the proceedings commenced on January 30, 2023. In accordance with the Rules, paragraph 5, the initial due date for Response was February 19, 2023. Upon request of Respondent, the Response due date was extended to February 23, 2023, under paragraph 5(b) of the Rules. The Response was filed with the Center on February 16, 2023, and an amended Response was filed with the Center on February 17, 2023.

Complainant filed a supplemental filing on February 24, 2023. Respondent filed objections to Complainant's supplemental filing on the same day.

The Center appointed Lawrence K. Nodine as the sole panelist in this matter on March 3, 2023. The Panel finds that it was properly constituted. The Panel has submitted the Statement of Acceptance and Declaration of Impartiality and Independence, as required by the Center to ensure compliance with the Rules, paragraph 7.

The Panel elected to exercise its discretion to consider Complainant's supplemental filing and, accordingly, also considered Respondent's Reply.

4. Factual Background

Complainant is a global provider of information solutions and human resources business process outsourcing services for businesses, governments and consumers. Complainant was originally incorporated in 1913 in Georgia in the United States, and now operates or has investments in 24 countries in North America, Central and South America, Europe, and the Asia Pacific regions. Complainant owns three United States trademark registrations for the mark EQUIFAX (Registration Nos. 1027544, registered on December 16, 1975, 1045574, registered on August 3, 1976, and 1644585, registered on May 14, 1991) (hereinafter the "Mark"). Complainant also operates the website associated with the domain <equifax.com>, which it registered on February 21, 1995. Complainant's services include a credit reporting service that provides consumers with a summary of their information that has been reported to credit bureaus by lenders and creditors.

On September 7, 2017, Complainant announced that it had experienced a massive data breach that exposed the personal information of 147 million people.

Complainant had registered the domain <equifaxsecurity2017.com> on August 22, 2017. That domain name resolved to a website providing consumers information on whether their information had been exposed in the data breach.

Respondent registered the Disputed Domain Name on September 7, 2017. For ten days after registration, the Disputed Domain Name resolved to a website that displayed two features—an absurdly silly music video[1] and a scrolling marquee message that read as follows:

> What the frick did you just fricking say about me, you little b*tch? I'll have you know I graduated top of my class in the Purple republic and 4chan, and I've been involved in numerous secret raids on club penguin, and I have over 300 confirmed DDOSES[2] I am trained in ddosing and I'm the top hackerin the entire 4chan armed forces. You are nothing to me but just another target. I will ddos you the frick out with precision the likes of which has never been seen before on this Internet, mark my fricking words. You think you can get away with saying that sh*t to me over the Internet? Think again, fricker. As we speak, I am contacting my secret network of spies and neckbeards across the 4chans and deep web and your IP is being traced right now so you better prepare for the storm, maggot. The storm that wipes out the pathetic little thing you call your internet. You're fricking booted, Cody. I can be anywhere, anytime, and I can ddos you in over seven hundred ways, and that's just with my bare

[1] "https://www.youtube.com/watch?v=aTBlKRzNf74" viewed March 15, 2023.

[2] DDOSES is an acronym for a "distributed denial-of-service attack." " In computing, a denial-of-service attack (DoS) is a cyber-attack in which the perpetrator seeks to make a machine network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to a network. Denial of service is typically accomplished by flooding the target machine or resource with superfluous requests in an attempt to overload the systems . . . in a distributed denial-of-service attack (DDOS), the incoming traffic flooding the victim originates from many different sources." See "https://en.wikipedia.org/wiki/Denial-of-service_attack", viewed March 15, 2023.

> hands. Not only am I extensively trained in unarmed hackingbut I have access to the entire arsenal of the hacker known as Anonymous and I will use it to its full extent to wipe your miserable butt off the face of the Internet, you little sh*t. If only you could have known what unholy retribution your little "clever" comment was about to bring down upon you, maybe you would have held your fricking tongue. But you couldn't, you didn't, and now you're paying the price, you goddamn idiot. I will sh*t fury all over you and you will drown in it. You're fricking booted, kiddo.

(hereinafter referred to as the "Hacker Message"). After about ten days, Respondent deleted the content of the webpage. Since September 16, 2017, the Disputed Domain Name has simply redirected to Complainant's website at <equifaxsecurity2017.com>.

5. Parties' Contentions

A. Complainant's Original Filing

Complainant contends that the Disputed Domain Name is confusingly similar to its EQUIFAX Mark, as the Disputed Domain Name incorporates the entirety of the Mark, only adding the word "security" to the end of it.

Next, Complainant states that Respondent has no rights or legitimate interests in the Disputed Domain Name, as Respondent is not affiliated with Complainant, Respondent has never been commonly known by the Disputed Domain Name, and Complainant has not assigned, granted, licensed, sold, transferred or in any way authorized Respondent to register or use the EQUIFAX Mark. Complainant further alleges that Respondent has never used, or made preparations to use, the Disputed Domain Name in connection with a *bona fide* offering of goods or services and instead only uses the Disputed Domain Name to redirect Internet visitors to Complainant's own website. Complainant further contends that redirecting to Complainant's website is not a legitimate use.

Additionally, Complainant submits that Respondent registered and continues to use the Disputed Domain Name in bad faith. Complainant contends that its Mark is famous or widely known because it is protected by 221 trademark registrations in at least 56 jurisdictions worldwide, and the Mark has been used in commerce for almost 48 years. As such, Complainant states that it is implausible that Respondent was unaware of Complainant and its rights in the Mark when it registered the Disputed Domain Name. Complainant categorizes Respondent's registration as opportunistic bad faith. Complainant further alleges that Respondent continues to use the Disputed Domain Name in bad faith because redirection of the Disputed Domain Name is evidence that Respondent is exploiting the renown of Complainant's Mark.

B. Respondent's Original Filing

Respondent does not dispute that the Disputed Domain Name is confusingly similar to Complainant's Mark.

Respondent does not dispute that it redirects to Complainant's website or make any effort to defend this redirecting as a *bona fide* good faith use.

Instead, Respondent contends that he registered the Disputed Domain Name on the day of Complainant's announcement of its security breach in order to post a website criticizing Complainant's lack of security. Respondent states that prior to the current redirect to Complainant's website, the Disputed Domain Name resolved to a webpage posting a link to the music video "Night of Fire" by Hinoi Team. Therefore, Respondent claims that his use of the Disputed Domain Name constitutes a legitimate noncommercial, and fair use of the domain name, and falls within the safe harbor of Policy, paragraph 4(c)(iii).

Respondent argues that he did not register and use the Disputed Domain Name in bad faith. Respondent claims that he registered the Disputed Domain Name to express his opinion on Complainant's handling of its 2017 security failure, not for any commercial gain.

Respondent further states that less than ten days after his registration of the Disputed Domain Name, he redirected the Disputed Domain Name to Complainant's website, which now provides consumers with information on how to obtain details of the Equifax Class Action Settlement.

C. Complainant's Supplemental Filing

In its Supplemental Filing, Complainant states that it was not until the Response was filed that Complainant learned that Respondent had previously used the Disputed Domain Name in connection with an active website for approximately ten days in September 2017, following Complainant's disclosure of a cybersecurity incident.

Complainant argues that the Hacker Message that appeared on the website associated with Disputed Domain Name during this ten-day period falsely made it appear as if Complainant had been successfully targeted by a hacker who threatened Internet users that they were "being traced right now." Complainant states that the Hacker Message did not actually criticize Complainant as alleged by Respondent, and therefore, undermines Respondent's claim of fair use. Complainant also contends that this message caused further, unwarranted alarm and damage, including tarnishment, to Complainant's EQUIFAX Mark, thereby constituting bad faith registration and use of the Disputed Domain Name.

D. Respondent's Reply to Complainant's Supplemental Filing

In its Reply to Procedural Order No. 1, Respondent argues that it never sought any commercial gain; that he has rights under the First Amendment to the United States Constitution to criticize Equifax; that Complainant has known of Respondent's fair use for many years and includes copies of emails that Complainant sent to Respondent in November and December 2017 objecting to the registration of the Disputed Domain Name; and that Complainant's arguments ignore the website's "most prominent feature, namely the Hanoi Team music video . . . Said video (which was set to autoplay) immediately signaled the message that the website was not to be taken seriously, with the obvious implication that Equifax did not take its solemn responsibility to safeguard the personal financial information of nearly every adult American seriously."

6. Discussion and Findings

A. Laches and Delay

It is unclear whether Respondent contends that Complainant's five-year delay in bringing this action should bar relief. Assuming he does, the Panel rejects to contention. "Panels have widely recognized that mere delay between the registration of a domain name and the filing of a complaint neither bars a complainant from filing such case, nor from potentially prevailing on the merits." WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Third Edition ("WIPO Overview 3.0"), section 4.17.

B. Identical or Confusingly Similar

The Panel finds that Complainant's trademark registrations establish that it has rights in the EQUIFAX Mark. Because the Disputed Domain Name incorporates Complainant's Mark entirely, it is confusingly similar to Complainant's registered Mark. Respondent's addition of the term "security" does not prevent a finding of confusing similarity. See WIPO Overview 3.0, section 1.8. (See also *Universal Services of America, LP d/b/a Allied Universal v. Carolina Rodrigues, Fundacion Comercio Electronico*, WIPO Case No. D2022-4222 (finding <alliedsecuritycontracts.com> confusingly similar to complainant's ALLIED UNIVERSAL and ALLIED UNIVERSAL SECURITY SERVICES marks).)

C. Rights or Legitimate Interests

Respondent argues that it registered the Disputed Domain Name for the purpose of publishing material meant to ridicule Complainant's lack of security, and that this use constitutes fair use of the Disputed Domain

Name, specifically noncommercial free speech.

Respondent abandoned its purported criticism content no later than September 16, 2017, which was a mere ten days after the Disputed Domain Name was registered. For more than five years since then, Respondent has been content to redirect Internet visitors without comment or criticism to Complainant's <equifaxsecurity2017.com> website. "Panels tend to assess claimed respondent rights or legitimate interests in the present, *i.e.*, with a view to the circumstances prevailing at the time of the filing of the complaint. . . . Panels will often also consider any evidence of previous legitimate use under the third UDRP element." WIPO Overview 3.0, section 2.11.

Therefore, the Panel finds that the relevant use for purposes of Policy paragraph 4(c)(ii) is the current use which has prevailed for all but a ten days following the registration of the Disputed Domain Name, for more than five years. The Panel finds that the current use—redirecting to Complainant's site—is not a legitimate use as is described in more detail below. A respondent cannot insulate illegitimate current use by pointing to some period of prior legitimate use, especially where, as here, the purported fair use lasted only ten days and the current use (redirecting) has occurred for more than five years – and moreover where it is not even clear that the prior (10-day) use was unequivocally legitimate or fair use (*i.e.*, the silly video was not accompanied by any commentary on Complainant's security practices – to the contrary it contained the misleading (or ambiguous at best) Hacker Message).

Respondent's abandonment after ten days of the initial content also belies his contention that Complainant filed this action because it wanted to suppress Respondent's criticism. Respondent says that he himself deleted the purportedly critical content after only ten days, which would have been weeks before Complainant sent an email on November 15, 2017, complaining about the registration of the Disputed Domain Name.

The Panel will consider Respondent's contention that the content on the website for ten days after registration reflects fair use commentary in the next section when the Panel considers whether Respondent registered and used the Disputed Domain Name in bad faith. It is sufficient to note here, however, that, even if the initial ten day content were considered relevant to the rights and legitimate use issue, the Panel would reject Respondent's fair use contention for the reasons explained in the next section.

Accordingly, the Panel finds that Complainant has established the second element under paragraph 4(a) of the Policy.

D. Registered and Used in Bad Faith

The Panel finds that Respondent registered the Disputed Domain Name in bad faith. Respondent acknowledges that he was fully aware of and targeted Complainant. Respondent's redirection of visitor's to Complainant's website is evidence of bad faith registration. WIPO Overview 3.0, section 3.1.3; *Government Employees Insurance Company ('geico') v. Angela Barlow*, WIPO Case No. D2020-0841 (redirection to Complainant demonstrates targetting and bad faith registration)

Respondent ignores the redirection evidence and contends that his *initial* intent was to mock Complainant with an absurd music video joke and criticize Complainant's lax security. The Panel agrees that if Respondent's original intent when he registered the Disputed Domain Name was to criticize Complainant, then this could indicate good faith registration even if Respondent stopped the critical content after ten days. But the Panel rejects this interpretation of the facts and finds bad faith registration based on the original content displayed for ten days.

The Disputed Domain Name is nearly identical to Complainant's Mark, which supports an inference that Respondent intended to impersonate or at least attract traffic meant for Complainant. The Disputed Domain Name does not contain any signal that it is not affiliated with Complainant. While panels have routinely recognized a respondent's claim to a legitimate interest under paragraph 4(c)(iii) of the Policy where the criticism is genuine and noncommercial, see WIPO Overview 3.0, section 2.6.1, the domain names at issue in those cases generally incorporate negative terms, (*e.g.* "sucks," or "hate," etc.) which signal to consumers

that these domain names are not affiliated with the respective complainants. The registration of a domain name reflecting the trademark of a third party, even where the domain name consists of a trademark plus an additional term, will not constitute fair use if it effectively impersonates or suggests sponsorship or endorsement by the trademark owner. See *The First Baptist Church of Glenarden v. Melvin Jones*, WIPO Case No. D2009-0022. *Dover Downs Gaming & Entertainment, Inc. v. Domains By Proxy, LLC/ Harold Carter Jr, Purlin Pal LLC,* WIPO Case No. D2019-0633.

In this case, the Disputed Domain triggers an inference of affiliation because the Disputed Domain Name does not signal that Respondent is engaging in a critique of Complainant, but incorporates the term "security," which is directly connected to Complainant's business. See *Puravankara Projects Limited v. Saurabh Singh*, WIPO Case No. D2014-2054.

Furthermore, there was no critical commentary about Equifax or its security procedures on Respondent's website. The silly music video is admittedly absurdly funny, but it makes no statement about Equifax that the Panel can detect. And the scrolling Hacker Message makes no critical commentary about Equifax's lax security.

Instead of offering critical commentary, the Panel finds that when Respondent registered the Disputed Domain Name, he intended to imitate an Equifax website that had been compromised by hackers. The scrolling Hacker Message on the website threatened Internet visitors that they were exposed to same risk of being hacked ("your IP is being traced right now"). That is the explicit message of the scrolling text.

The Panel finds that the Hacker Message is evidence that Respondent intended to further tarnish Complainant's reputation, and convey to visitors that, above and beyond the widely reported data breach, hackers had taken complete control of an Equifax website. This was bad faith, especially in the context of Complainant's widely publicized data breach. See WIPO Overview 3.0, section 3.12 (tarnishment may be evidence of bad faith).

Respondent moreover asserts that the scrolling Hacker Message was just "random text designed to immediately signal that the site . . . was not to be taken seriously, with the obvious implication that Complainant Equifax did not take its responsibility for customer security seriously". Especially noting the fact that a security breach of Complainant's systems had in fact occurred, the Panel finds nothing in the Hacker Message to suggest that the message should not be taken seriously.

It is significant that, as Respondent repeatedly emphasizes, the Disputed Domain Name was registered on the same day that Complainant's data breach was disclosed to the public. Millions of people were likely searching online for information about the breach. If they landed upon Respondent's website, many would have viewed the scrolling Hacker Message as evidence that Complainant had been hacked. Victims of Complainant's data breach would likely take Respondent's hacker threats and boasts seriously – on an incorrect assumption that it was a site of Complainant – rather than dismiss them as Respondent suggests.

In effect, Respondent was impersonating a website operated by Complainant that had been hacked at a time when Internet visitors were likely concerned about the vulnerability of Complainant's Internet assets.

While the Panel concedes that the funny video cuts in Respondent's favor, it is not enough to overcome the menacing message of the Hacker Message and the inference of affiliation created by the nearly identical domain name. If the silly music video were the only content on the webpage, then a visitor might laugh and move on. But the silly music video was seen in conjunction with the aggressive Hacker Message and the nearly identical domain name. The combined effect would be ambiguous at best and, more likely, menacing to many Internet visitors. Lastly, as mentioned, the fact that this content lasted on the website at the Disputed Domain Name for only a period of ten days before the use of the Disputed Domain Name changed to an illegitimate redirection and stayed that way for more than five years also supports a finding of bad faith on the part of Respondent.

Respondent emphasizes that it had no commercial motive and derived no financial benefit from the Disputed Domain Name. Conduct that tarnishes Complainant and its trademarks is evidence of bad faith. There is no requirement that the tarnishment be commercially motivated.

Accordingly, because the Panel finds that Respondent intended to tarnish Complainant's reputation, it holds that Respondent registered the Disputed Domain Name in bad faith.

The Panel also finds that Respondent used the Disputed Domain Name in bad faith.

First, Respondent's redirection to Complainant's website is bad faith use. WIPO Overview 3.0, section 3.1.4. Although the Panel addresses Respondent's initial ten-day use, the Panel emphasizes that it views the current redirection as the dominant and relevant use for the purpose of evaluating bad faith use. Accordingly, the Panel finds that Respondent has used and continues to use the Disputed Domain Name in bad faith.

Respondent's initial ten-day Hacker Message was also bad faith use because it was intended to further damage the goodwill associated with Complainant's Mark. See *Wagamama Limited v. Park Hae Dong, Hae Dong Limited* WIPO Case No. D2008-0301 ("[T]he nature of the website is such that linkage with a complainant's mark could reasonably be supposed to tarnish that mark then the result would be bad faith use").

The Panel finds that Complainant has established the third element under paragraph 4(a) of the Policy.

7. Decision

For the foregoing reasons, in accordance with paragraphs 4(i) of the Policy and 15 of the Rules, the Panel orders that the Disputed Domain Name, <equifaxsecurity.com>, be transferred to Complainant.

/Lawrence K. Nodine/
Lawrence K. Nodine
Sole Panelist
Date: April 1, 2023