ARBITRATION
AND
MEDIATION CENTER

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

ADMINISTRATIVE PANEL DECISION
International Business Machines Corporation (IBM) v. Chait, Mitch, IBMS
Case No. D2023-2911

1. The Parties

The Complainant is International Business Machines Corporation (IBM), United States of America ("United States"), internally represented.

The Respondent is Chait, Mitch, IBMS, United States, internally represented.

2. The Domain Name and Registrar

The disputed domain name <ibms.com> is registered with Network Solutions, LLC (the "Registrar").

3. Procedural History

The Complaint was filed with the WIPO Arbitration and Mediation Center (the "Center") on July 6, 2023. On July 7, 2023, the Center transmitted by email to the Registrar a request for registrar verification in connection with the disputed domain name. On July 11, 2023, 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 (Perfect Privacy, LLC) and contact information in the Complaint. The Center sent an email communication to the Complainant on July 13, 2023, providing the registrant and contact information disclosed by the Registrar, and inviting the Complainant to submit an amendment to the Complaint. The Complainant filed an amendment to the Complaint on July 13, 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 the Respondent of the Complaint, and the proceedings commenced on July 19, 2023. In accordance with the Rules, paragraph 5, the due date for Response was August 12, 2023. The Response was filed with the Center on August 13, 2023. The Complainant submitted a supplemental filing with attachments on August 26, 2023. The Respondent submitted a supplemental filing on August 28, 2023, and subsequently requested an opportunity to reply in greater detail to materials in the Complainant's supplemental filing. This was granted in Administrative Panel Order Number One, and the Respondent submitted a supplemental filing on

September 17, 2023.

The Center appointed W. Scott Blackmer as the sole panelist in this matter on August 29, 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.

4. Factual Background

The Complainant is a corporation established under the laws of the State of New York, United States and headquartered in Armonk, New York, United States, with shares publicly traded on the New York Stock Exchange. The Complainant produces a wide array of information technology products and also offers consulting services, doing business globally with nearly 300,000 employees.

Operating as "International Business Machines" since 1924, the Complainant has used the initials "IBM" to brand its goods and services since at least 1925, as demonstrated by photos included in the record. The record also shows that the IBM mark is widely recognized throughout the world. In 2022, when the Complainant was listed as the 49th largest company on the Fortune US 500 list and the 168th largest company on the Fortune Global 500 list, IBM was ranked the 18th most valuable global brand by BrandZ and the 18th best global brand by Interbrand. The IBM mark achieved similarly high rankings in 2021 and 2020 and in earlier years. The Complainant spends over USD 1 billion annually marketing goods and services under the IBM mark through multiple channels, including its principal website at "www.ibm.com" (the "Complainant's website"). The mark has frequently been the target of cybersquatters, and panelists have regularly recognized its renown, as in *International Business Machines Corporation v. Sadaqat Khan*, WIPO Case No. D2018-2476:

"The panel is of the opinion that the Complainant's trademark has a strong reputation and is widely known throughout the world."

The Complainant has trademark registrations for IBM in numerous countries, including the following subsisting United States registrations:

Mark	Registration Number	Registration Date	Goods and Services
IBM (standard characters)	640606	January 29, 1957	Magnetic recording tape (and accessories); IC 9
IBM (standard characters)	1058803	February 15, 1977	Data processing, dictating, photocopying machines and supplies, printer and copier paper and ink, computer programs, typewriters, medical equipment, adhesives; maintenance services, consulting, programming, engineering, and education services; IC 1, 2, 3, 4, 7, 9, 10, 16, 28, 37, 41, 42
IBM (stylized letter)	1205090	August 17, 1982	Data processing and word processing equipment and supplies, copying machines and printers and supplies, computer systems, terminals, memories, medical equipment, typewriters, dictating equipment, composing machines, related supplies, maintenance, consulting, education, engineering, leasing office space; IC 1, 2, 7, 9, 10, 16, 37, 41, 42

IBM (standard characters)	1694814	June 16, 1992	Financing information handling systems, financial investment services; IC 36
IBM (stylized letters)	3002164	September 27, 2005	Batteries, blank magnetic computer discs and tapes, chips, circuit boards, computer hardware, computer software; IC 9
IBM (stylized letters)	4181289	December 21, 2010	Wall plaques, hand tools, computer software, data media, protective cases, headsets, miniature lamps and similar personal items, books and other printed matter, briefcases and travel bags, sweatshirts and other clothing, lanyards and badges, confectionary, advertising and consultancy services, conference organization services; IC 9, 16, 18, 20, 21, 22, 24, 25, 28, 35, 41

The Registrar reports that the disputed domain name was created on December 15, 1998, and was registered in the name of a domain privacy service. After receiving notice of the Complaint in this proceeding, the Registrar identified the underlying registrant as the Respondent Mr. Chait of the organization "IBMS", listing a postal address in Las Vegas, Nevada, United States and "[***]@greenfence.com" as a contact email address.

The Response attaches documents and the declarations of Mr. Chait and his accountant and colleague Kelvin Harris showing that IBMS LLC is a Delaware (United States) limited liability company formed in April 2011 and headquartered in Las Vegas, Nevada, United States. Mr. Chait is the managing member of IBMS and is also the proprietor of Greenfence, LLC and Greenfence Consumer, LLC. The Respondent states that IBMS is an acronym for "Intelligent Behavior Management System", and the record shows that IBMS holds related patents for such a system issued by the United States Patent and Trademark Office (USPTO) in 2014.

The Declaration of Mr. Chait attached to the Response indicates that the Respondent IBMS operates or invests in a variety of technology businesses and has used the disputed domain name over the years to host or redirect to websites related to those businesses. Immediately prior to this dispute, the disputed domain name redirected to a website operated by the Respondent at <greenfence.io> advertising the launch of the Respondent's "GiFT" financial technology platform, a business now operating at "www.gftmaker.com". The disputed domain name and the domain names <greenfence.com> and <greenfence.io> are not associated with active websites at the time of this Decision. The Respondent indicates that its control over the disputed domain name was disabled following the Complainant's communications with the Registrar in April 2023, as described further below.

The Complaint does not mention earlier use of the disputed domain name, but the Respondent provides records from the Internet Archive's Wayback Machine, and the Panel has examined screenshots from that source of the websites and landing pages to which the disputed domain name resolved over time. In 1999 the disputed domain name was used for a website operated by K&M Software Design, Ltd, advertising software called Investigative Business Management System (IBMS). The disputed domain name was then parked for many years on landing pages with pay-per-click ("PPC") third-party advertising portals, consistent with the Chait Declaration to the effect he acquired the disputed domain name after the formation of IBMS LLC in 2011. From approximately May 2014 through early April 2023, the disputed domain name resolved to the website of Greenfence, LLC (the "Greenfence website"), advertising "Greenfence" business software, which evolved from a food industry supply chain certificate and compliance tracking program to a blockchain platform adapted for a variety of supply chain and consumer services. The website ultimately displayed a "TM" symbol next to the name GREENFENCE, and the online database of the USPTO shows that this mark was registered to the Respondent IBMS on December 11, 2018. By March and early April 2023, the Greenfence website consisted only of a landing page displaying the name "Greenfence", a figurative logo,

copyright and cookies notices, and a LinkedIn social media link. After that, the disputed domain name redirected to the Respondent's website at <greenfence.io> to advertise the Respondent's new "fintech" (financial technology) business.

The Complainant sent a cease-and-desist email to the Respondent through the Registrar on April 18, 2023, stating that the disputed domain name infringed on the IBM trademark and redirected to the Respondent's website at <greenfence.io>. The email demanded that the Respondent transfer the disputed domain name to the Complainant. The Complainant says there was no reply, but the Respondent attaches its May 3, 2023, email denying that there is a basis for a trademark infringement claim given the "historical record" of IBMS. (The Complainant's supplemental filing acknowledges this reply but characterizes it as "terse".)

Meanwhile, the Complainant's cyber threat intelligence team reported an apparent phishing attack in March 2023 using the email address "[***]@br.ibms.com". Two emails were sent from that address to one of the Complainant's customers in March 2023, purportedly from a person with a name corresponding to an actual IBM employee and with "-IBM" following her name, from "LA IBM Certified Pre Owned". The emails referred to offers and asked for the customer's personal email and bank details to facilitate payment. One of the emails included a footer with the Complainant's trademarked logo, the initials IBM in stylized letters. In its supplemental filing, the Complainant provides additional evidence about the phishing emails: metadata reveal that they were sent from an IP address identified on spam lists as associated with a botnet network that distributes malware.

The Respondent furnishes correspondence with the Registrar establishing that the Respondent in 2022 and 2023 has had only one email box for the disputed domain name, which it has not used, and no email box with a name corresponding to the one used in the phishing attack on the Complainant.

5. Parties' Contentions

A. Complainant

The Complainant asserts that the disputed domain name is identical or confusingly similar to its registered IBM mark, incorporating the mark in its entirety and adding the letter "s". The Complainant states that it has never authorized the Respondent or another third party to register the disputed domain name. The Complainant contends that there is no evidence that the Respondent is using the disputed domain name for a *bona fide* offering of goods or services, using it illegitimately instead for fraudulent emails in a phishing scheme.

The Complainant argues that this use of the disputed domain name also signifies bad faith within the meaning of the Policy, as the Respondent was clearly aware of the Complainant's well-established mark and targeted at least one of the Complainant's customers. In addition, the Complainant argues that it should benefit from a presumption of bad faith as the disputed domain name merely adds a letter to the Complainant's famous IBM mark. As further indications of bad faith, the Complainant points to the Respondent's registration through a domain privacy service and its establishment of mail servers for the disputed domain name that could be used for phishing purposes.

B. Respondent

The Respondent contends that the disputed domain name is based on its company name, IBMS, which was registered as a company in 2011, and is not identical to the Complainant's IBM trademark. The Respondent contends as well that this is not confusingly similar to the IBM mark, which does not appear prominently in Internet searches for "IBMS". The Respondent observes that other organizations also use domain names that legitimately differ by a single letter from "IBM" because of their initials, operating websites, for example, at "www.ibmc.com", "www.ibmi.com", "www.ibml.com", "www.ibms.us", and "www.ibms.org".

The Respondent asserts rights and legitimate interests in using its company name for a corresponding domain name, which it was using in connection with the *bona fide* offering of commercial services until the disputed domain name was disabled as a result of the Complainant's demand to the Registrar. The Respondent points to the history of this legitimate use of the disputed domain name, since the establishment of IBMS as a company in 2011, to support its denial of any intent to exploit the Complainant's trademark. The Respondent states that the Complainant is not mentioned on any of the websites associated with the disputed domain name. The Respondent emphasizes that it has conducted its own business with reputable companies and organizations, including "household name" clients such as T-Mobile and PepsiCo, while its affiliate Greenfence is associated with the Consumer Goods Forum.

The Respondent also denies any involvement in the March 2023 phishing attacks on the Complainant, of which the Respondent was not aware until receiving the Complaint in this proceeding. The Respondent details its subsequent communications with the Registrar and highlights the Registrar's confirmation that the Respondent does not have an email mailbox corresponding to the one from which the phishing emails originated, as well as the Complainant's own internal security report indicating that the emails originated from a known botnet.

The Respondent, which is not represented by counsel, does not expressly claim reverse domain name hijacking ("RDNH") under the Rules, paragraph 15(e), but the Respondent makes detailed allegations of knowing misrepresentations, failure to investigate, harassment, and bad faith on the part of the Complainant. The Panel construes these as tantamount to a request for a finding of RDNH.

6. Discussion and Findings

Paragraph 4(a) of the Policy provides that in order to divest a respondent of a domain name, a complainant must demonstrate each of the following: (i) the domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and (ii) the respondent has no rights or legitimate interests in respect of the domain name; and (iii) the domain name has been registered and is being used in bad faith. Under paragraph 15(a) of the Rules, "[a] Panel shall decide a complaint on the basis of the statements and documents submitted and in accordance with the Policy, these Rules and any rules and principles of law that it deems applicable".

6.1 Preliminary Matter: Supplemental Filings

Both parties submitted supplemental filings with attachments. While much of the content is ultimately immaterial to the Decision or reargues points made in the initial filings, the supplemental filings include some new, relevant information on the phishing attacks and the Respondent's use of the disputed domain name, or in reply to claims of bad faith raised in the Response. The Panel accepts the filings for consideration on these issues.

6.2 Substantive Issues

A. Identical or Confusingly Similar

The first element of a UDRP complaint "functions primarily as a standing requirement" and entails "a reasoned but relatively straightforward comparison between the complainant's trademark and the disputed domain name". WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Third Edition ("WIPO Overview 3.0"), section 1.7.

The Complainant holds trademark registrations for IBM. The disputed domain name is confusingly similar, adding a final letter "s", which is often simply read as a plural. The mark is readily recognizable in the disputed domain name (see *id.*). As usual, the addition of the Top-Level Domain ".com" may be disregarded as a standard registration requirement (see *id*. section 1.11.1).

The Panel finds that the disputed domain name is confusingly similar to the Complainant's mark for purposes of the first Policy element.

B. Rights or Legitimate Interests

Paragraph 4(c) of the Policy gives non-exclusive examples of instances in which a respondent may establish rights or legitimate interests in a domain name, by demonstrating any of the following:

(i) before any notice to it of the dispute, the respondent's use of, or demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a *bona fide* offering of goods or services; or

(ii) the respondent has been commonly known by the domain name, even if it has acquired no trademark or service mark rights; or

(iii) the respondent is making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.

Because a respondent in a UDRP proceeding is in the best position to assert rights or legitimate interests in a domain name, it is well established that after a complainant makes a *prima facie* case, the burden of production on this element shifts to the respondent to come forward with relevant evidence of its rights or legitimate interests in the domain name. See WIPO Overview 3.0, section 2.1.

The Complainant has demonstrated trademark rights, and at the time the Complaint was filed the disputed domain name was used to redirect to a website without a corresponding name and arguably for phishing emails. This suffices to establish a *prima facie* case. Hence, the burden of production passes to the Respondent on this Policy element.

The Respondent claims rights and legitimate interests based on its company name and its longstanding commercial use of the disputed domain name. The Complainant correctly observes in its supplemental filing that "IBMS" does not feature on the Respondent's former Greenfence website or the other websites to which the disputed domain name resolved or redirected. The Panel notes that "IBMS" also does not appear on the Greenfence social media page, and while the USPTO database shows that IBMS LLC has registered a GREENFENCE trademark, it evidently has not registered an "IBMS" trademark. Thus, although the Respondent has been using the disputed domain name for websites serving its affiliated businesses, the Complainant's argument on its face has merit, that the Respondent has not demonstrated that it is "commonly known" as "IBMS". Moreover, the Complainant relies heavily on the argument that the Respondent must have been aware of the world-famous IBM mark and meant to exploit it with a confusingly similar domain name, as evidenced by the March 2023 phishing attacks, and this undercuts the Respondent's claims to be engaged in a *bona fide* use of the disputed domain name.

The Panel finds that the balance of the evidence on the phishing attacks weighs in the Respondent's favor. The Respondent denies involvement in the phishing attacks, and this denial is credible. The Respondent is a substantial company registered more than 12 years ago with a patent and trademark portfolio. It has been actively using the disputed domain name for a decade in connection with legitimate business activities including the provision of digital trust certificates and secure blockchain services to major corporations in regulated industries. It is highly unlikely that the Respondent would suddenly engage in an illicit phishing scheme targeting one of the Complainant's customers to obtain its bank account details. The Registrar confirms that (a) only one email mailbox was established for the disputed domain name, (b) it was not used in 2022 or in 2023 to date, and (c) it does not correspond to the email address used for the phishing attacks. Further, the Complainant's own internal information security report indicates that the phishing attack originated from an IP address associated with a known botnet. Thus, on this record the evidence does not support the Complainant's inference that the Respondent launched the March 2023 phishing attacks. Moreover, although the Respondent has not used the disputed domain name for an "IBMS" website, the Respondent's claims to rights or legitimate interests nevertheless appear to meet the conditions of the

Policy, paragraph 4(c)(i), which requires use in connection with a *bona fide* offering of goods or services. The Policy does not require that the use be in the form of a website labelled with the disputed domain name. The Respondent has demonstrated its use of the disputed domain name for a succession of affiliated businesses for many years, until its control of the disputed domain name was disabled when this dispute arose. IBMS LLC is clearly not merely a sham company registered to facilitate cybersquatting and trademark exploitation. The company has functioned for more than 12 years and actually holds patents and a registered trademark (for GREENFENCE). This may suffice to establish that the Respondent is "commonly known" by its company name for purposes of the Policy, paragraph 4(c)(ii). In any event, the Respondent's commercial service offerings using the disputed domain name, before any notice of the dispute, would serve to establish its rights or legitimate interests so long as they were not determined to be a pretext for bad faith exploitation of the Complainant's mark, a possibility more fully explored in the following section of the Decision.

C. Registered and Used in Bad Faith

The Policy, paragraph 4(b), furnishes a non-exhaustive list of circumstances that "shall be evidence of the registration and use of a domain name in bad faith", including the following:

"(iv) by using the domain name, you [respondent] have intentionally attempted to attract, for commercial gain, Internet users to your [respondent's] web site or other online location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your [respondent's] website or location or of a product or service on your website or location."

The Complainant argues that its mark is well-known and long-established, such that the Respondent must have been aware of it, as evidenced by registering (or later acquiring) a domain name with a slight misspelling of the distinctive mark and then using it for phishing attacks impersonating an employee of the Complainant.

The Respondent has not denied prior awareness of the Complainant's mark but denies any intent to exploit it and denies any involvement in the phishing attacks. On this record, the Panel finds the Respondent's denials credible.

The Panel finds persuasive evidence that the Respondent was not the source of the phishing attacks, as detailed in the preceding section. The fact that the Respondent activated mail servers for its account does not suffice to establish bad faith, where the Respondent has legitimate reasons for using the disputed domain name and the evidence shows that the phishing attacks on the Complainant did not originate from an email account established by the Respondent.

On balance, it also seems improbable that the Respondent registered its company name in 2011 and then acquired a corresponding domain name based on the acronym for its software-based solutions that the Respondent then patented and commercialized, all as part of a scheme to attack the Complainant's mark by misleading relatively sophisticated potential corporate clients. As the Respondent observes, there are other legitimate businesses and organizations that similarly have initials (and domain names) that differ from the Complainant's mark by having another letter following "IBM". It is unlikely that the Complainant's suggested scheme of misdirection would be effective, and the Complainant has not shown that any of the websites associated with the disputed domain name imitated, targeted, or competed with the Complainant, or that the disputed domain name resulted in actual confusion.

The Complainant's other arguments for bad faith are similarly unpersuasive. The fact that the Respondent registered the disputed domain name through a domain privacy service is not, by itself, indicative of bad faith. There are several good reasons for doing so, such as avoiding spam and phishing email attacks. And the Respondent has in fact responded to the Complaint in this proceeding and to the Complainant's earlier cease-and-desist demand, despite the Complainant's initial claim to the contrary (which the Complainant in its supplemental filing conceded was a mistake).

In sum, the Panel does not find bad faith in the registration and use of the disputed domain name on this record and concludes that the Complainant has not established the third element of the Complaint.

Given this finding, the Panel also concludes that the Respondent prevails on the second element of the Complaint.

7. Decision

For the foregoing reasons, the Complaint is denied.

8. Reverse Domain Name Hijacking

Paragraph 15(e) of the UDRP Rules provides that, if "after considering the submissions the panel finds that the complaint was brought in bad faith, for example in an attempt at Reverse Domain Name Hijacking ('RDNH') or was brought primarily to harass the domain-name holder, the panel shall declare in its decision that the complaint was brought in bad faith and constitutes an abuse of the administrative proceeding".

The Respondent did not request such a finding here but made specific allegations of negligence, misrepresentations, harassment, and bad faith in the investigation, filing and continued prosecution of the Complaint. The Complainant has had an opportunity to address these allegations in its supplemental filing.

Reverse Domain Name Hijacking is defined under the UDRP Rules as "using the UDRP in bad faith to attempt to deprive a registered domain-name holder of a domain name". Mere lack of success of a complaint is not sufficient to find Reverse Domain Name Hijacking. See WIPO Overview 3.0, section 4.16. A finding of RDNH is warranted, for example, when a panel finds that the complainant (especially one represented by counsel) should have recognized that it could not succeed on one of the three elements of the complaint under any fair interpretation of the available facts or brings a complaint based "on only the barest of allegations without any supporting evidence" (id.).

Here, the Complainant inadequately investigated the underlying facts. The disputed domain name was registered more than 24 years before the Complaint was filed, which should have suggested that some basic research was in order to determine when it was acquired by the current registrant and how the registrant has used it since. The Complaint did not refer to the more than 250 archived screenshots of the disputed domain name, merely asserting (erroneously) that the disputed domain name had only been used for a redirect to <greenfence.io> and for phishing emails. The Complainant also did not mention (until its supplemental filing) the fuller report from the Complainant's own security team indicating that the March 2023 phishing emails came from an IP address associated with a botnet on spam lists, thus casting doubt on the Complainant's theory that the Respondent sent the phishing emails. However, the Complainant was responding to a blatant spoofing email attack using the disputed domain name and did not necessarily have to accept the Respondent's denials of involvement. The IBM mark is well known and frequently attacked by cybersquatters and fraudsters, as evidenced in numerous UDRP decisions. On balance, the Panel finds that the Complainant's prosecution of the Complaint was ill conceived and poorly executed but does not represent harassment or bad faith as described in Rule 15(e). Therefore, the Panel declines to enter a finding of RDNH.

/W. Scott Blackmer/
W. Scott Blackmer
Sole Panelist
Date: September 24, 2023