

ADMINISTRATIVE PANEL DECISION

HAI Group v. Name Redacted

Case No. D2026-2474

1. The Parties

The Complainant is HAI Group, United States of America ("United States"), represented by ZeroFox, United States.

The Respondent is Name Redacted.¹

2. The Domain Name and Registrar

The disputed domain name <hiagroup.com> is registered with Unstoppable Domains Inc. (the "Registrar").

3. Procedural History

The Complaint was filed with the WIPO Arbitration and Mediation Center (the "Center") on June 8, 2026. On June 9, 2026, the Center transmitted by email to the Registrar a request for registrar verification in connection with the disputed domain name. On the same date, 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 (Registration Private / Unstoppable Privacy Service LLC) and contact information in the Complaint. The Center sent an email communication to the Complainant on June 11, 2026, 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 June 16, 2026.

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").

¹As discussed by the Panel in the Decision, the disputed domain name appears to have been identified by a third party when sending email, without the Respondent's involvement or direct use of the disputed domain name. In light of this, the Panel has redacted the Respondent's name from this Decision. The Panel has authorized the Center to transmit Annex 1 to the Registrar as part of the order in these proceedings and has indicated that Annex 1 to this Decision shall not be published due to the exceptional circumstances of this case. See *Banco Bradesco S.A. v. FAST-12785241 Attn. Bradescourgente.net / Name Redacted*, WIPO Case No. [D2009-1788](#).

In accordance with the Rules, paragraphs 2 and 4, the Center formally notified the Respondent of the Complaint, and the proceedings commenced on June 17, 2026. In accordance with the Rules, paragraph 5, the due date for the Response was July 7, 2026. The Response was filed with the Center on July 7, 2026.

The Center appointed Jeremy Speres as the sole panelist in this matter on July 10, 2026. 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 issued Procedural Order No. 1 on July 13, 2026, inviting the Complainant to provide the Panel with the alleged phishing email referenced in the Complaint by July 18, 2026, and giving the Respondent until July 23, 2026, to respond. The Complainant responded on July 17, 2026, and the Respondent responded on July 23, 2026.

4. Factual Background

The Complainant has, since 1987, traded under the HAI GROUP mark as a United States-based insurance enterprise, operating as a property-casualty insurance provider to public and affordable housing authorities across the United States.

The Complainant's HAI GROUP mark is registered in the United States under Trademark Registration No. 4256911 HAI GROUP (device) in classes 36, and 41, having a registration date of December 11, 2012, and a first use in commerce date of February 29, 2004.

The Complainant's primary website is operated from the Complainant's domain name <haigroup.com> (registered in 2001).

The disputed domain name was registered on May 26, 2015, and presently resolves to a parked page stating: "This domain is registered, but may still be available."

The Respondent is a domain name investor based in Germany.

5. Parties' Contentions

A. Complainant

The Complainant contends that it has satisfied each of the elements required under the Policy for a transfer of the disputed domain name.

Notably, the Complainant contends that the Respondent registered and used the disputed domain name in bad faith with actual knowledge of the Complainant and its HAI GROUP mark. It argues that the disputed domain name is an obvious typosquatted version of its mark and domain name and was used in a phishing scheme that impersonated a named employee, reproduced genuine contact details and billing information, and sought to divert invoice payments to a fraudulent bank account, conduct falling squarely within paragraph 4(b)(iv) of the Policy.

B. Respondent

The Respondent contends that the Complainant has not satisfied the elements required under the Policy for a transfer of the disputed domain name.

Notably, the Respondent denies any bad faith, asserting that the disputed domain name is a generic three-letter acronym combined with the descriptive word "group", acquired and passively held as a legitimate domain investment for over 11 years without any knowledge of the Complainant. The Respondent argues

that the alleged phishing email was the product of external email header spoofing using a Gmail account, not the disputed domain name, which allegedly never had Mail Exchange (“MX”) records and was technically incapable of sending or receiving email. The Respondent requests a finding of Reverse Domain Name Hijacking (“RDNH”).

6. Discussion and Findings

A. Identical or Confusingly Similar

It is well accepted that the first element functions primarily as a standing requirement. The standing (or threshold) test for confusing similarity involves a reasoned but relatively straightforward comparison between the Complainant’s trademark and the disputed domain name. WIPO Overview of WIPO Panel Views on Select UDRP Questions ([“WIPO Overview 3.1”](#)), section 1.7.

The Complainant has shown rights in respect of a trademark or service mark for the purposes of the Policy. [WIPO Overview 3.1](#), section 1.2.1.

The Panel finds the mark is recognizable within the disputed domain name. Accordingly, the disputed domain name is confusingly similar to the mark for the purposes of the Policy. [WIPO Overview 3.1](#), section 1.7. To the extent that the design elements of the Complainant’s mark are incapable of representation in domain names, these elements are generally disregarded for purposes of assessing identity or confusing similarity. [WIPO Overview 3.1](#), section 1.10. A domain name which consists of a common, obvious, or intentional misspelling of a trademark, as in this case with “hai” versus “hia”, is considered by UDRP panels to be confusingly similar to the relevant mark for purposes of the first element. [WIPO Overview 3.1](#), section 1.9.

The Panel finds the first element of the Policy has been established.

B. Rights or Legitimate Interests

In light of the Panel’s findings in relation to the third element below, there is no need to consider the second element.

C. Registered and Used in Bad Faith

The only direct evidence of any bad faith usage of the disputed domain name tendered by the Complainant was an alleged phishing email, sent on May 8, 2026, from somebody impersonating an actual employee of the Complainant. That email appears to be a case of classic Business Email Compromise (“BEC”) in which the sender impersonated an employee of the Complainant, asking a client of the Complainant to settle fictitious invoices.

The problem for the Complainant, however, is that it is clear from the face of that email that it involved email spoofing and was apparently not sent from the disputed domain name. The sender’s display name was set to include the Complainant’s employee’s name as well as an email address at the disputed domain name within the text of the display name itself, whilst the actual sending address of that email was a Gmail address. This was clear from the face of the forwarded email that the Complainant attached to the Complaint.

In Procedural Order No. 1, the Panel invited the Complainant to provide it with the original May 8, 2026, email, including its full, unaltered Simple Mail Transfer Protocol (“SMTP”) headers, so that the Panel could confirm its provenance. The Complainant provided this, and the Panel was able to confirm, from a reading of the headers, that the email was sent from a Gmail address and not the disputed domain name. There is therefore no evidence in the record that either the disputed domain name was used to send, or that the Respondent sent, the phishing email.

In its response to Procedural Order No. 1 the Complainant attempts to explain why the disputed domain name or the Respondent may still have been the source of the phishing email despite the technical evidence showing otherwise. The Complainant stated:

“Had the actor behind Annex 12 [the original phishing email] wished merely to impersonate Ms. [...] as effectively as possible, the Complainant's actual corporate domain, haigroup.com, was available to be typed into that field at no greater effort and with no risk of a telltale misspelling. Instead, the message used the precise transposed-letter string that happens to be a domain name independently registered and controlled by the Respondent. An unconnected third party choosing this particular typographical variant, rather than the correct domain readily available to anyone impersonating the Complainant, is a detour requiring its own explanation, one the Response does not attempt to supply.”

This does not assist the Complainant. There is simply no evidence that the disputed domain name was involved in the phishing email, other than as part of a display name, which any third party could have inserted without controlling the disputed domain name. Speculating on the motivations or identity of the party behind the phishing email (the “phisher”) does not assist the Complainant, especially where the standard of proof is the balance of probabilities.

In any event, despite the Respondent not raising this point, the Panel considers that there are a number of plausible reasons why a phisher might choose not to spoof the Complainant's actual domain name. One possible explanation is the following. The Panel has independently checked the publicly accessible Domain Name System (“DNS”) records for the Complainant's corporate domain name <haigroup.com> and notes that the Complainant has included Sender Policy Framework (“SPF”) DNS records. SPF is an email authentication method that checks if a sending mail server is permitted to send email for a specific domain name. It works through DNS text records listing approved IP addresses, and it helps prevent email spoofing. The phisher may well have been aware of this and may have wanted to avoid triggering the Complainant's SPF policy, which could have resulted in the recipient of the phishing email's (the Complainant's client's) own mail servers rejecting the phishing email as having been sent from an unauthorized mail server.

In the absence of any direct evidence of bad faith usage of the disputed domain name, the Complainant is essentially left with the similarities between the disputed domain name and its HAI GROUP mark. They are undoubtedly similar, however, there are two difficulties here for the Complainant. Firstly, it has not established that its mark is well known and has not put forward any evidence showing why the Respondent, based in Germany, would or should have known of the Complainant's mark. As the Respondent points out, the Complainant's own website is geographically restricted and does not permit users from outside of the United States to access it, making it less likely that any reputation in the Complainant's mark could have extended to the Respondent's jurisdiction.

Secondly, “hia” is a three-letter acronym with broad application, and there is nothing in the record contradicting the Respondent's claim that he acquired the disputed domain name as an investment for purposes of resale. With the Respondent having held the disputed domain name for 11 years, the absence of any direct evidence of bad faith over such a long period undermines the Complainant's claims of targeting.

The Panel finds the third element of the Policy has not been established.

D. Reverse Domain Name Hijacking

Paragraph 15(e) of the 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 RDNH or 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 mere lack of success of the complaint is not, on its own, sufficient to constitute reverse domain name hijacking. [WIPO Overview 3.1](#), section 4.16.

The Respondent requested a finding of RDNH, contending that the Complainant, assisted by a specialist cybersecurity firm, failed to undertake basic technical due diligence that would have revealed the absence of

any email infrastructure associated with the disputed domain name and the alleged phishing email's true origin from an external Gmail account.

The Complainant is indeed represented by a specialist cybersecurity firm, and it could well be asked whether they may have appreciated the points around spoofing and SPF addressed above. Nevertheless, the phishing email was prepared with cunning and the display name versus sending address issue was, by design, easy to miss.

Although the Complainant was professionally represented, the Panel is not persuaded that the deficiencies in the Complaint were so obvious that the filing of the Complaint itself constituted an abuse of process.

The Panel declines to find RDNH accordingly.

7. Decision

For the foregoing reasons, the Complaint is denied.

/Jeremy Speres/

Jeremy Speres

Sole Panelist

Date: July 28, 2026