ARBITRATION
AND
MEDIATION CENTER

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

ADMINISTRATIVE PANEL DECISION

Groupement d'Achats des Opticiens Lunetiers - GADOL v. Philippe Caturegli
Case No. DAD2025-0004

1. The Parties

The Complainant is Groupement D'achats Des Opticiens Lunetiers – GADOL, France, represented by GUIU IP, France.

The Respondent is Philippe Caturegli, United States of America, self-represented.

2. The Domain Name and Registrar

The disputed domain name <optic2000.ad> is registered with Andorra Telecom (the ".ad Registry") through Namecheap, Inc. (the "Registrar").

3. Procedural History

The Complaint was filed with the WIPO Arbitration and Mediation Center (the "Center") on December 11, 2025. On December 12, 2025, the Center transmitted by email to the .ad Registry a request for registrar verification in connection with the disputed domain name. On December 15, 2025, the .ad Registry 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 Purposes) and contact information in the Complaint.

The Center sent an email communication to the Complainant on December 15, 2025, providing the information disclosed by the .ad Registry, and inviting the Complainant to amend the Complaint. The Complainant filed an amended Complaint on December 19, 2025.

The Center verified that the Complaint as amended satisfies the formal requirements of the .ad Dispute Resolution Policy ("adDRP" or "Policy"), the Rules for .ad Dispute Resolution Policy (the "adDRP Rules") and the Supplemental Rules of the WIPO Arbitration and Mediation Center for .ad ("WIPO adDRP Supplemental Rules").

In accordance with the adDRP Rules, paragraphs 2 and 4, the Center formally notified the Respondent of the Complaint, and the proceedings commenced on December 26, 2025. In accordance with the adDRP Rules, paragraph 5, the due date for Response was January 15, 2026. The Response was filed with the Center on January 9, 2026.

The Center appointed Jeremy Speres as the panelist in this matter on January 22, 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 adDRP Rules, paragraph 7.

The Panel issued Procedural Order No. 1 on January 28, 2026, inviting the Respondent to comment, by February 2, 2026, on why he chose to send pre and post-Complaint security disclosures to a particular email address, and why he believes the Complainant received these communications. The Complainant was given until February 7, 2026, to respond to any response from the Respondent. The Respondent responded on January 28, 2026. The Complainant responded on February 3, 2026. The Respondent responded to the Complainant's response on February 10, 2026.

The Panel issued Procedural Order No. 2 on February 16, 2026, inviting the Respondent to confirm, by February 21, 2026, his unconditional offer to transfer the disputed domain name to the Complainant, and, if so, inviting the Complainant to inform the Center whether these proceedings should be suspended pending settlement discussions by February 26, 2026. The Respondent responded on February 19, 2026, requesting that the Panel proceeds to issue a decision on the merits.

The Panel issued Procedural Order No. 3 on February 20, 2026, inviting the Complainant to comment on the Respondent's submission of February 10, 2026, by February 25, 2026. The Complainant did not respond to Procedural Order No. 3.

4. Factual Background

The Complainant, founded in 1969, trades in optical goods and services under the OPTIC 2000 mark, having over 1,200 stores in France. The Complainant's OPTIC 2000 mark has been recognized as being well known in France by a panel in a prior case under the Uniform Domain Name Dispute Resolution Policy ("UDRP"). See *Groupement d'achats des opticiens lunetiers-GADOL contre Multiramys*, WIPO Case No. D2012-2254.

The Complainant's OPTIC 2000 mark is registered under, amongst others, French Trademark Registration No. 3558031 OPTIC 2000 in classes 9, and 35, having an effective registration date of February 22, 2008.

The Complainant owns the domain name <optic2000.com>, registered in 1997, which it uses for its website.

The Respondent, founder of the cybersecurity consultancy Seralys, is a cybersecurity professional, claimed to have over 25 years of experience in offensive security, vulnerability research, and infrastructure security. The Respondent's research has been reported in popular cybersecurity publications, including the well-known Krebs on Security blog. A particular area of research that the Respondent has focussed on is the security vulnerabilities caused by internal domain name collisions, particularly those involving Microsoft's Active Directory service which is widely used in Microsoft Windows networks. In essence, internal domain name collisions occur when organizations use domain names for internal network infrastructure (like Active Directory) which have not been registered in the global, public Domain Name System ("DNS"). If such domain names are subsequently registered in the public DNS by unauthorised third parties, serious security risks can arise, such as credential leakage, leaking of internal DNS queries and thus exposure of internal network topologies, and interception of internal communications.

The disputed domain name was registered on December 17, 2024, and resolves to a blank webpage.

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 disputed domain name was registered and has been used in bad faith for the purpose of preventing the Complainant from registering the disputed domain name corresponding to its trademark and for the purpose of disrupting the business or activities of the Complainant. The Complainant argues that Andorra, which is the country whose country-code Top-Level Domain ("ccTLD") forms part of the disputed domain name, borders its primary territory of France, and that the disputed domain name's registration will prevent it from developing its business in Andorra and will confuse customers who travel between Andorra and France. The Complainant relies on the doctrine of passive holding to the extent that the disputed domain name is not used.

B. Respondent

The Respondent claims that the Complainant has not satisfied all of the elements required under the Policy for a transfer of the disputed domain name. Notably, the Respondent contends as follows.

As part of his research into internal domain name collisions, the Respondent routinely engages in Internet-wide scanning activities searching for self-signed digital identity certificates, which often expose internal domain name collisions. In December 2024, whilst engaged in such scanning, the Respondent identified an Internet-exposed service operated by the Complainant's network which utilised the disputed domain name as an internal domain name for an Active Directory service, which the Respondent noted had not been registered in the public DNS.

The Respondent proceeded to register the disputed domain name for two purposes. Firstly, to prevent malicious third parties from themselves registering the disputed domain name and exploiting the associated security vulnerabilities. Secondly, to seek to affirm identification of the affected organization and facilitate responsible disclosure through controlled observation of any traffic directed to the disputed domain name.

The Respondent made good faith efforts at contacting the Complainant, as follows:

On March 7, 2025, after confirming the affected organization's identity, the Respondent attempted to email the Complainant using the email address "security@optic2000.com" which he assumed (apparently incorrectly – see discussion under the third element) may be a domain name in the Complainant's network. The Respondent's email fully disclosed the vulnerability, and, amongst other things, unconditionally offered to transfer the disputed domain name to the Complainant.

On December 2, 2025, after the Complainant had not responded to the foregoing email, the Respondent reported the vulnerability to the French national Computer Emergency Response Team (CERT-FR).

On December 15, 2025, the Respondent was copied to the Center's correspondence to the Complainant notifying the Complainant of the Respondent's identity. This was the first time that the Respondent was informed that the Complaint had been filed. On the same day, the Respondent responded to the Center, with the Complainant's counsel in copy, stating:

"The domain was registered in good faith as part of legitimate security research relating to internal domain name collision risks, and solely to prevent potential malicious abuse of a domain observed to be in use within internal networks.

In this context, multiple attempts were made to contact Optic2000 / Audioptic directly to report the apparent misconfiguration. We also notified the French CERT (ANSSI) in accordance with responsible disclosure practices. To date, no response has been received from the Complainant regarding these reports."

On December 19, 2025, not having received any response from the Complainant, the Respondent sent a follow up email to "security@optic2000.com", again explaining the vulnerability and offering to unconditionally transfer the disputed domain name to the Complainant. Again, no response from the Complainant was forthcoming.

The Respondent claims that his conduct constitutes legitimate noncommercial fair use given that he has not sought to exploit the Complainant's trademark, has not used the disputed domain name in any commercial way, and his research serves the public good.

The Respondent claims that his conduct was not in bad faith as it was motivated by technical cybersecurity research and a desire to protect against malicious use, not by any intent to target the Complainant's trademark.

The Respondent asks for a finding of Reverse Domain Name Hijacking ("RDNH") on the basis that the Complainant had actual, prior knowledge of the Respondent's legitimate purpose and failed to respond to repeated attempts at collaborative resolution.

6. Discussion and Findings

A. Identical or Confusingly Similar

For the purposes of paragraph 4(a)(i) of the Policy, the term "Relevant Identifier" encompasses trademarks that are validly registered either in Andorra before the Oficina de Marques i Patents del Principat d'Andorra ("OMPA") or in a foreign jurisdiction.

The Complainant has shown rights in respect of the OPTIC 2000 trademark for the purposes of the Policy.

The entirety of the Complainant's registered trademark is reproduced within the disputed domain name, apart from the space. Spaces within a trademark can be disregarded for purposes of assessing identity (*Novomatic AG v. Oleg Bakanach*, WIPO Case No. D2020-1667). Accordingly, the disputed domain name is identical to the mark for the purposes of the Policy. WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Third Edition ("WIPO Overview 3.1"), section 1.7.[1]

The Panel finds that the Complainant has satisfied the requirements of paragraph 4(a)(i) of the Policy.

B. Registered or Used in Bad Faith

This case presents a relatively unique scenario in the context of the UDRP and its progeny such as the Policy. The Panel has found only one prior case under the UDRP where a panel explicitly, albeit *obiter*, recognised a legitimate interest flowing from genuine cybersecurity research. In *Universal Services of America, LP d/b/a Allied Universal v. Mansor Almossa*, WIPO Case No. D2023-2288, the panel stated:

"Again, the Panel notes that the evidentiary record is devoid of any plausible explanation or legitimate need for Respondent to send emails to, or receive emails from, anyone using the disputed domain name, which Complainant has persuasively argued creates a likelihood of confusion with Complainant's human resources department. To be perfectly clear, while such an explanation or legitimate need may arguably exist, as in the

[1] The Panel notes that the Policy is largely derived from the UDRP and considers it appropriate to refer to UDRP authorities.

case of cybersecurity research, there is nothing in this particular case to suggest anything other than Respondents' lack of rights or legitimate interests."

The Panel has only been able to find two prior cases that substantively dealt with defences based on genuine cybersecurity endeavours, specifically:

Facebook, Inc. and Instagram, LLC v. WhoisGuard Protected, WhoisGuard, Inc. / Phishing Operations, Wombat Security Technologies, WIPO Case No. D2020-3218 ("Wombat"); and

Aetna Inc. v. On behalf of help-aetna.com owner / Whois Privacy Service / Manager / Knowbe4, WIPO Case No. D2021-1565 ("Aetna").

Both of these cases involved legitimate cybersecurity consultancy businesses intentionally registering domain names that used the complainants' trademarks for purposes of conducting training for their clients' employees in combatting email-based phishing. In each case, the domain names in question were used to send emails impersonating the complainants for purposes of testing and educating the respondents' clients' employees in the dangers of email-based phishing.

The two cases followed largely similar fact patterns, apart from the fact that in *Wombat*, the domain names resolved to a landing page pointing out that they are used for security awareness training, and hyperlinking to the respondent's own website. In *Aetna*, the domain name did not resolve to any website.

Wombat was decided in favour of the complainant, with the panel finding that the respondent's actions were to be considered in bad faith given that, amongst others, the domain name had been used to create confusion which led users to the respondent's own commercial website for the respondent's commercial benefit.

Aetna was decided in favour of the respondent, with the panel finding that, because the respondent reasonably believed that what it was doing constituted legitimate fair use, and because this intention was backed up by precautionary measures and a unique and restricted form of use, it could not be said that the registration of the domain name was in bad faith. The panel's decision was expressly informed by the fact that the respondent had not used the domain name to bring the respondent commercial gain, by, for example, directing users to its own commercial website (*contra Wombat*).

In the present case, the Respondent registered the disputed domain name in the course of cybersecurity research and specifically offered to transfer the disputed domain name to the Complainant. Based on the available record, the Respondent's offer to transfer did not refer to any conditions or charges. The Respondent does not appear to have been acting under a paid commercial contract and conducted this research of his own accord. The disputed domain name has not been used to resolve to any active website nor to drive traffic to the Respondent's own platforms in any way. As such, and in the absence of any evidence to the contrary, his conduct was apparently not motivated by commercial gain, and can be distinguished from the conduct of the respondents in both *Wombat* and *Aetna*, who both registered the domain names in the course of undertaking paid commercial services, and, in one of those cases, the respondent used the domain names to link to its own commercial website.

The Respondent made multiple efforts to contact the Complainant (albeit problematic, as discussed below), being transparent about his actions, the details of the vulnerability, and his willingness to transfer the disputed domain name to the Complainant. He went as far as reporting the matter to the French cybersecurity authorities when he did not hear from the Complainant. If he had nefarious intentions for the disputed domain name, that would be an odd thing to do.

The Respondent's reputation as a bona fide and skilled cybersecurity researcher has been established by his publications and press coverage in the field, including, in particular, in the area of cybersecurity research that covers the specific vulnerability that was present in the Complainant's internal network. The Complainant in fact recognised the vulnerability in its network when it stated in its Amended Complaint: "Indeed, an Active Directory is configured on optic2000. When the Complainant's computers attend to communicate with 'optic2000' Active Directory, there is a risk that they attempt to connect to the disputed domain name servers, resulting to data leaks. The Complainant took the necessary measures to limit this risk, but any change in the configuration of the disputed domain name could create a new risk."

In the circumstances, it appears to the Panel that the Respondent was in his mind acting as a proverbial Good Samaritan. He asked nothing in return for the considerable expertise, time and effort that he spent. His actions caused no harm to the Complainant nor its trademark. This is consistent with industry best practices in cybersecurity vulnerability disclosure. The Panel has independently determined that one authoritative source of such best practices is the CERT Guide to Coordinated Vulnerability Disclosure maintained by the CERT Coordination Center (CERT/CC), which is part of the Software Engineering Institute at Carnegie Mellon University. Of its core principles, harm reduction is the first.[2] Contrary to harming the Complainant, the Respondent's actions may have benefited it. The Complainant does not appear to have been aware of the vulnerability prior to the Respondent bringing it to its attention, and the Complainant is fortunate that a good faith, ethical hacker discovered the vulnerability before a bad faith one.
The Respondent's conduct was, therefore, benevolent, which is the antithesis of bad faith.

The Panel has also independently determined that at least one cybersecurity industry body has specifically considered best practices for cybersecurity professionals who make use of "look-alike" domain names. The Messaging, Malware and Mobile Anti-Abuse Working Group ("M3AAWG") published its "Best Practices for Use of Look-Alike Domains for Security Purposes" paper in September 2025.[3] The recommendation most relevant to the Respondent's situation is the fifth one:

"Consider contacting the trademark owner for awareness, coordination, and agreement to help avoid confusion, takedown efforts, unnecessary costs, wasted time, and animosity. In a cooperative solution, the registrant of a look-alike domain name can transfer ownership of the look-alike domain to the trademark owner, who can then point the look-alike domain to the researcher's nameservers of choice. This allows the trademark owner to permit use of the domain, while retaining some control."

This the Respondent attempted to do.

There is, however, one disquieting aspect of the Respondent's attempts at contacting the Complainant. Both before and after the Complaint was filed, and before and after the Center copied the Respondent to its correspondence notifying the Complainant of the Respondent's identity, the Respondent disclosed the vulnerability and his registration of the disputed domain name to the Complainant by sending an email to "security@optic2000.com". The Respondent in his Response stated that this is the Complainant's "designated security email address", although no evidence was provided to this effect.

In Procedural Order No. 1, the Panel invited the Respondent to comment on why he chose to use that particular email address for his disclosure, why he claimed that it was the Complainant's designated security address, and why he believes the Complainant received these communications. The Respondent's response was to claim that the email address "security@optic2000.com" was selected because it constitutes the internationally recognized default contact point for security vulnerability disclosures when an organization does not publish a specific security contact. The Respondent relied, in this regard, on four industry standards, specifically: RFC 2142 (May 1997), RFC 9116 (April 2022), ISO/IEC 29147:2018, and FIRST (Forum of Incident Response and Security Teams) Guidelines.

---

[2] See "www.certcc.github.io/CERT-Guide-to-CVD/topics". In accordance with its powers articulated inter alia in paragraphs 10 and 12 of the Rules, the Panel is entitled to conduct limited independent research into matters of public record. WIPO Overview 3.1, section 4.8.
[3] See "www.m3aawg.org/lookalike-domains-bcp-2025".

Insofar as the Panel can tell,[4] these standards do indeed recommend using "security@domain" as a designated email address for receiving vulnerability disclosures. However, the recommendations are specifically for the receiving party to implement; they recommend that those who might need to receive vulnerability disclosures (network operators, software vendors etc) should provision such an email address. They do not, however, state that reporters of vulnerabilities are entitled to blindly assume that such an email address is actually provisioned or designated when there is no evidence of that, in the form of, for example, designated security contact information displayed on a website or in a "security.txt" file.[5] They also do not state that reporters of vulnerabilities are entitled ignore contact details that are actually published, as in this case.

In the present case, contrary to his assertion in the Response, the Respondent has not been able to point to any evidence showing that the Complainant actually designated "security@optic2000.com" as its security email address, that that email address was provisioned on its network, or that the Complainant received those emails. The Complainant's website makes no such designation, it does not include a "security.txt" file, and Internet searches reveal no such designation either. On the contrary, the Complainant's website has a contact form and lists various other email addresses for the purposes of contacting the Complainant, including on its "Contact" page at "www.optic2000.com/contact" and in its Privacy Policy at "www.optic2000.com/politique-de-confidentialite-des-donnees".

It therefore seems odd that the Respondent would have chosen to report the vulnerability to the Complainant using an email address for which there was no evidence to suggest that it had been designated or even provisioned by the Complainant, rather than using an email address that the Complainant had in fact designated, and in a rather obvious place.

The Respondent may have had concerns about confidentiality and the vulnerability falling into the wrong hands if he used a general contact email address or form, as he states in his response to the Complainant's response to Procedural Order No. 1. That is a reasonable concern. However, the Respondent could quite easily have avoided this risk by sending a communication to the general contact email address or using the contact form, asking to be put in touch with a security contact, pointing out, in general terms only, that he had discovered a vulnerability. At least one prominent cybersecurity training company recommends just this. The Infosec Institute states as follows in its guide on reporting security vulnerabilities:

"[M]any companies have a 'Contact Us' form on their website or other contact information for their customers. Reach out this way explaining that you've discovered a potential security issue and would like to contact the IT or security team. However, don't provide details at this point in case the message falls into the wrong hands."[6]

The CERT Guide to Coordinated Vulnerability Disclosure referenced above also provides guidance for vulnerability reporters for finding contact details for disclosure purposes. Various methods are suggested, including: "Many vendors have a 'Contact Us' form on their web site that can be used to make initial contact… Sometimes the best way to reach a vendor is to make a phone call."[7]

It seems to the Panel that if the Respondent had used the obvious contact details actually provided on the Complainant's website rather than presuming, without any evidence, that the Complainant had provisioned the "security@optic2000.com" email address, then he would have greatly increased the probability of the Complainant actually receiving the disclosure along with the Respondent's offer to transfer the disputed

---

[4] ISO/IEC 29147:2018 is not freely available online, and the Respondent did not provide a copy. However, on the Respondent's own version, this standard recommends that "organizations should provide a security contact point, commonly implemented as security@[domain]". Thus, it is a standard for the receiving party to implement, and not a standard giving vulnerability reporters licence to blindly assume that it has in fact been implemented, as discussed in the body of the Decision above.

[5] RFC 9116 (April 2022) introduced a new standard for designating security contacts using a file named "security.txt" located in the "/.well-known/" directory of a website. See "www.rfc-editor.org/rfc/rfc9116". This file was not present on the Complainant's website.

[6] See "https://www.infosecinstitute.com/resources/vulnerabilities/how-to-report-a-security-vulnerability-to-an-organization/".

[7] See "www.certcc.github.io/CERT-Guide-to-CVD/howto/initiation/find_vendor_contact".

domain name. If he had done so, the Complaint may well never have been filed, these proceedings may well have been unnecessary, and the matter could well have been resolved amicably.

Nevertheless, although this may have been remiss of the Respondent, and although this is relevant to the Respondent's request for a finding of RDNH (addressed below), the Panel does not consider that it is sufficient, on its own, to characterise the Respondent's conduct as being in bad faith. The balance of the Respondent's actions, including reporting the vulnerability to the French cybersecurity authorities before the Complaint was filed, shows very clearly that the Respondent was acting in good faith.

In his Response, the Respondent reiterated his unconditional willingness to transfer the disputed domain name to the Complainant. In light of this and his earlier emails sent to the Complainant in which that offer was made, the Panel issued Procedural Order No. 2, asking the Respondent to confirm whether that offer stood, and if so, inviting the Complainant to request suspension of the proceedings for purposes of settlement. The Respondent's response was to state:

"The Respondent already declined a settlement offer from the Complainant's counsel on January 16, 2026, particularly given that the Complainant proceeded with this complaint despite having full knowledge of our security research and the vulnerability we disclosed. At this stage, the Respondent wishes to remain consistent with this decision, and therefore respectfully requests that the Panel proceed to issue a decision on the merits.

That said, we hereby confirm that the Respondent will transfer the domain name unconditionally and immediately following the Panel's decision."

The Respondent has therefore refused to transfer the disputed domain name to the Complainant until a decision on the merits has been made. This may, upon initial impression, seem contradictory to the Respondent's earlier offers to transfer the disputed domain name to the Complainant, and it may, superficially at least, call the Respondent's motives into question.

However, the Panel finds that it is perfectly plausible that the Respondent may genuinely want an affirmative finding on the merits to clarify, for future purposes, that his vulnerability research activities involving domain names are legitimate. The Panel also notes that the Respondent has requested a finding of RDNH, and it is perfectly plausible that the Respondent genuinely wants a finding of RDNH after the Respondent has been put to the costs and inconvenience of filing a Response, possibly to deter future complaints in similar circumstances. The Panel therefore does not consider the Respondent's refusal to transfer the disputed domain name to the Complainant at this late stage in the proceedings as pointing to bad faith on his part.

The Panel finds that the Respondent's registration and initial use of the disputed domain name was undertaken as part of legitimate cybersecurity research. However, the Panel notes that the Respondent has repeatedly and unconditionally offered to transfer the disputed domain name to the Complainant and has confirmed that he has no ongoing interest in retaining it.

Panels have the authority to order transfer of a disputed domain name on the basis of a unilateral consent from a respondent alone. See WIPO Overview 3.1, paragraph 4.10. This is on the basis of the powers afforded to a panel in terms of paragraph 10 of the Rules to conduct these proceedings "in such manner as it considers appropriate in accordance with the Policy and these Rules" and to "ensure that the administrative proceeding takes place with due expedition". See *Williams-Sonoma, Inc. v. EZ-Port*, WIPO Case No. D2000-0207.

The Panel considers that the Respondent's repeated offers of transfer, including his last filing offering to transfer the disputed domain name after the Decision is issued, amount to a unilateral consent. With a view to conducting these proceedings expeditiously, and in order to avoid placing the Complainant in the invidious position of potentially having to refile this Complaint at additional cost should the promised transfer not occur, the Panel considers that it is in the interests of justice to order the transfer now.

The Panel has nevertheless chosen to comment substantively on the merits despite being entitled to order transfer on the basis of the consent alone, without doing so. This is because there is a broader public interest in establishing the legitimacy of responsibly conducted cybersecurity research, and considering the paucity of decisions under the UDRP and its progeny on this topic. See *GitHub, Inc. v. Chris Koepke*, WIPO Case No. D2023-2995, recognizing that it is appropriate to comment substantively where there is some public interest, despite there being a unilateral consent. Note that this would have limits e.g., as described in *Wombat* supra. See also WIPO Overview 3.1, section 4.10.

C. Reverse Domain Name Hijacking

The Respondent requested a finding of RDNH. His request is entirely predicated on the assumption that the Complainant was made aware of the Respondent's actions, through the Respondent's pre and post-Complaint vulnerability disclosure emails as well as his December 15, 2025 email, but decided to proceed with the Complaint anyway.

As addressed above, the Respondent sent his first vulnerability disclosure on March 7, 2025, to an email address at the Complainant's domain name without there being any evidence indicating that that email address was actually provisioned by the Complainant. The Complaint was filed with the Center on December 11, 2025. The fact that the Complainant did not refer to the that email in its Complaint, and did not take the Respondent up on the unconditional transfer offer (which would have been less costly and quicker than filing the Complaint) suggests that the Complainant did not actually receive these emails, probably because it had not provisioned the particular email address that the Respondent chose to use. The Complainant stated, in its response to Procedural Order No. 1, that it had in fact not provisioned that email address, and had in fact never received any emails prior to filing the Complaint. On balance of probabilities, without any evidence from the Respondent showing that the Complainant had actually provisioned or designated that email address, or showing that the Complainant actually received those emails, the Panel considers it more likely than not that the Complainant did not receive the Respondent's email of March 7, 2025, which was prior to the filing of the Complaint . That email then does not point to bad faith in the Complainant proceeding with the Complaint. Notably though, this may well have been different if the Respondent had used an email address or contact form actually designated by the Complainant, as addressed above.

That leaves the Respondent's December 15, 2025 email, the relevant parts of which are set out in the Respondent's Contentions in paragraph 5 above. That email did not contain the Respondent's offer to transfer the disputed domain name to the Complainant, nor did it contain any specific details of the particular vulnerability. Notably, that email was sent after the Complaint was filed. The Respondent argues in effect that his December 15, 2025 email should have given the Complainant pause and that the Complainant should not, thereafter, have persisted with an Amended Complaint. On the contrary, the Panel is not convinced that the Respondent's December 15, 2025 email contained sufficient information for the Complainant to assess whether the Respondent was indeed acting in good faith or not, especially given that the Respondent's offer to transfer the disputed domain name unconditionally was not included. It may or may not have been remiss of the Complainant not to pause and make further enquiries with the Respondent once it received the December 15, 2025 email, but given the paucity of information available to it at the time and the timeline it was given to file its Amended Complaint, the Panel does not believe that the Complainant was acting in bad faith in electing to proceed with the Amended Complaint.

In the circumstances, the Panel declines to enter a finding of Reverse Domain Name Hijacking.

7. Decision

For the foregoing reasons, in accordance with paragraphs 4(i) of the Policy and 14 of the Rules, the Panel orders that the disputed domain name <optic2000.ad> be transferred to the Complainant.

/Jeremy Speres/
Jeremy Speres
Panelist
Date: February 26, 2026