ARBITRATION
AND
MEDIATION CENTER

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

ADMINISTRATIVE PANEL DECISION
Equifax Inc. v. Domain Manager, Knowbe4
Case No. D2026-0176

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 Domain Manager, Knowbe4, United States, represented by Wilson Sonsini Goodrich & Rosati, United States.

2. The Domain Name and Registrar

The disputed domain name <equifax-credit.com> is registered with Amazon Registrar, Inc. (the "Registrar").

3. Procedural History

The Complaint was filed with the WIPO Arbitration and Mediation Center (the "Center") on January 16, 2026. On January 16, 2026, the Center transmitted by email to the Registrar a request for registrar verification in connection with the disputed domain name. On January 21, 2026, 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 (On behalf of equifax-credit.com owner, Identity Protection Service) and contact information in the Complaint. The Center sent an email communication to Complainant on January 22, 2026, providing the registrant and contact information disclosed by the Registrar, and inviting Complainant to submit an amendment to the Complaint. Complainant filed an amended Complaint on January 27, 2026.

The Center verified that the Complaint together with the amended 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 28, 2026. In accordance with the Rules, paragraph 5, the due date for Response was February 17, 2026. The Response was filed with the Center on February 17, 2026. Complainant requested that the proceeding be suspended on February 23, 2026. The proceedings were suspended until March 25, 2026, and reinstituted on March 26, 2026.

On March 25, 2026, Complainant submitted a supplemental filing to the Center and on March 27, 2026, Respondent sent an email to the Center requesting that Complainant's supplemental filing be disregarded or alternatively that Respondent be granted leave to file a response to such.

The Center appointed Georges Nahitchevansky, Robert A. Badgley, and Christopher S. Gibson as panelists in this matter on April 21, 2026. The Panel finds that it was properly constituted. Each member of 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.

On April 24, 2026, the Panel issued a procedural order accepting Complainant's supplemental filing and granting Respondent leave to file a response to such. On May 1, 2026, Respondent filed a response to Complainant's supplemental filing.

4. Factual Background

Complainant, Equifax, Inc., is a global data, analytics and technology company. Complainant provides various information solutions for businesses, governments and consumers as well as human resources business process automation and outsourcing services for employers, and consumer credit monitoring services under the name and mark EQUIFAX. Complainant owns a number of registrations for marks that consist of EQUIFAX around the world. Of particular relevance to this proceeding, Complainant owns registrations for EQUIFAX as a word mark in the United States in connection with its services (Registration Nos. 1,027,544, 1,045,574 and 1,644,585), the earliest of which issued to registration December 16, 1975. Complainant also owns and uses the domain name <equifax.com> for a website concerning Complainant and its services and which provides consumers with various offers to monitor their credit reports and for ID threat protection.

Respondent is based in the State of Florida in the United States. Respondent was founded in 2010 and was formerly a public company which was acquired by Vista Equity Partners in 2023. The Company works with a wide range of organizations worldwide, including Fortune 500 companies, well-known banks, credit unions and other financial institutions, as well as federal, state and municipal governments.

Respondent developed and operates a platform enabling organizations to assess, monitor, and minimize the threat of social engineering computer attacks. The platform is geared towards security awareness using cloud-based software, artificial intelligence, advanced analytics, and employee training. As part of the platform, Respondent employs a library of content for use by its corporate customers in simulated phishing attacks targeted to a customer's employees.

Respondent registered the disputed domain name on October 28, 2020. The disputed domain name resolves to an inactive website. Respondent claims that simulation exercises referencing the disputed domain name may be used by Respondent in connection with Respondent’s computer security training programs for its corporate clients in the form of simulated phishing attacks.

5. Parties’ Contentions

A. Complainant

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

Complainant maintains that it has strong rights in the EQUIFAX mark on account of its registration and longstanding use of the mark and that, as such, the EQUIFAX mark is well-known.

Complainant contends that the disputed domain name is identical or confusingly similar to the EQUIFAX mark as it contains the EQUIFAX mark in its entirety and merely adds the non-distinguishing, descriptive word “credit” at the tail of the disputed domain name.

Complainant argues that Respondent has no rights or legitimate interests in the disputed domain name as Complainant has never “assigned, granted, licensed, sold, transferred or in any way authorized Respondent to register or use the EQUIFAX trademark in any way”. Complainant further argues that Respondent lacks rights or a legitimate interest in the disputed domain name based on a prior UDRP decision in *Home Depot Product Authority v. Domain Owner / Knowbe4,* Forum Claim No. 1990823 (“*Home Depot v. Knowbe4*”), involving the use of the domain name <homedepotcustomercenter.com> by Respondent for simulated phishing attacks in connection with Respondent’s computer security training programs for its corporate clients. Finally, Complainant urges that Respondent lacks rights and legitimate interests as Respondent (i) is not commonly known by the disputed domain name and (ii) has failed to use the disputed domain name with an active website.

Lastly, Complainant asserts that Respondent has registered and used the disputed domain name in bad faith given that (i) Complainant's EQUIFAX mark is famous and/or widely known, and (ii) Respondent clearly was aware of Complainant's rights in the EQUIFAX mark when it opportunistically registered the disputed domain name for Respondent's profit. Complainant also cites the prior decision against Respondent in *Home Depot v. Knowbe4* as further proof of Respondent's bad faith and also notes that Respondent's lack of use of the disputed domain name for an active website or page is proof of “bad faith under the passive holding doctrine.“

B. Respondent

Respondent rejects Complainant's contentions.

Respondent explains that it has developed a “leading platform enabling organizations to assess, monitor, and minimize the threat of social engineering” and that for its platform it employs, and continuously refreshes, an expansive library of content for use by its corporate customers which reflects the latest range of social engineering threats. Respondent further explains that a key tenet of its platform “is the ability of its corporate customers to perform simulated social engineering exercise on their own employees as part of comprehensive training programs” in the form of simulated phishing emails using domain names “containing third-party names, marks, or variations thereof”.

Respondent emphasizes that it does not compete with Complainant, has never used the disputed domain name to divert customers of Complainant or used such in any way to disrupt Complainant's business, and has never offered to sell or transfer the disputed domain name to Complainant or anyone else.

Respondent asserts that it maintains the disputed domain name “as part of its repository of potential threat indicators, available for simulated phishing attacks” for its corporate clients. Respondent further explains that it takes a number of precautionary steps to ensure “that its intended use of the Disputed Domain Name in connection with security awareness training does not result in commercial harm”. In that regard, Respondent notes, inter alia, that (i) there is no website or content hosted at the disputed domain name and that anyone typing in the disputed domain name would receive an error message that the domain name cannot be found, and (ii) any employee of Respondent's customers who click on a link in a simulated phishing exercise involving the disputed domain name would receive “immediate feedback that they clicked on a simulated phishing exercise.“

Respondent concedes that the disputed domain name contains the EQUIFAX mark but maintains that the disputed domain name is neither identical nor confusingly similar to the Complainant’s trademark, given that it contains the suffix “-credit” and given the precautionary measures noted above taken by Respondent.

With regard to Respondent's rights or legitimate interests in the disputed domain name, Respondent argues that the disputed domain name is being used legitimately by Respondent in its stated field of activity of

providing “educational programs directed at Security Awareness”. Respondent further notes that security awareness through training exercises such as simulated spam phishing attacks is a legitimate activity. In that regard, Respondent contends that “utilizing a realistic simulation strictly for educational services, or vocational training” that includes the use of the disputed domain name as part of a training program is a fair use that is legitimate. Respondent also notes that in a previous UDRP case *Aetna Inc. v. On behalf of help-aetna.com owner / Whois Privacy Service / Manager / Knowbe4*, WIPO Case No. D2021-1565 (“*Aetna v. Knowbe4”*), that involved substantially similar circumstances as the matter at hand, Respondent prevailed.

Lastly, Respondent asserts that there is no evidence that Respondent registered and used the disputed domain name in bad faith given Respondent's use of the disputed domain name in a closed environment with precautionary measures for security awareness training. In particular, Respondent stresses that the simulated links used with the disputed domain name do not “direct to the domain itself, nor do they direct to a commercial sales page. Instead, they direct to an isolated educational landing page, or a standard message hosted on Respondent's secure servers”. Respondent also cites to the *Aetna Inc. v. Knowbe4* decision to further support its contentions that there has been no bad faith registration or use.

C. Parties Supplemental Filings

Neither the Policy nor the Rules provide a party with an automatic right to submit additional arguments or evidence. Under paragraph 10 of the Rules, panels enjoy broad powers for conducting administrative proceedings, provided that the parties are treated fairly and the proceedings are conducted expeditiously. Within this framework, a panel can determine within its sole discretion whether to admit or reject supplemental submissions, and, under paragraph 12 of the Rules, to request further statements or documents from either party. Here, the Panel after due deliberation, has decided to accept the parties' respective supplemental filings in the interest of obtaining a full record given the facts and issues underlying this dispute.

Complainant's Supplemental Filing

In Complainant's supplemental filing, Complainant argues that Respondent is a for-profit company and has mischaracterized its services as being for educational purposes. Complainant further argues that Respondent's use of the disputed domain name is meant to “enhance Respondent's ability to sell its expensive Security Awareness Training services”. Complainant makes additional arguments about the claimed effectiveness of Respondent's claimed phishing simulation exercises and notes that there is no need to register and use domain names based on the marks of others for such programs.

Complainant also questions the precautionary measures taken by Respondent and claims that the use of the disputed domain name causes initial interest confusion as it is meant to entice users to click on links that contain the disputed domain name. Complainant also maintains that Respondent could have taken numerous steps to possibly alleviate creating a likelihood of confusion with the EQUIFAX mark such as asking for Complainant's permission to register and use the disputed domain name. Complainant urges that Respondent's use of the disputed domain in connection with phishing simulation activities may result in some users – for example, even those who do not click on links containing the disputed domain name – associating Complainant with phishing or spam. Finally, Complainant adds that should the Panel bless Respondent’s actions (by denying a transfer of the disputed domain name), Respondent will be free to register additional domain names that contain the EQUIFAX mark, allowing ongoing confusion, damage, and forcing Complainant to incur further time and expense.

Respondents' Supplemental Filing

Respondent initially rejects Complainant's supplemental filing and asks that the Panel disregard such. Respondent reiterates that its registration of the disputed domain name is noncommercial and relates strictly to its cybersecurity education services. Respondent notes that consumers routinely pay for all kinds of educational services and that as such there is no basis for Complainant to claim that a for profit company cannot offer legitimate educational services.

Respondent notes that its educational simulated phishing attack program is effective, but notes that the effectiveness of such is irrelevant under the Policy as a respondent does not have to prove the necessity of its services in order to have a legitimate interest.

Respondent rejects Complainant's contentions of initial interest confusion as irrelevant as Respondent has taken "precautionary steps to ensure that its registration and passive holding of the disputed domain name in connection with security awareness training would not result in any commercial harm to Complainant". Respondent notes that it does not use hyperlinks to the disputed domain name and that employees who may click on links as part of a simulated phishing attack "are directed to a landing page, hosted on a separate domain, advising them they clicked on a simulated phishing exercise". Lastly, Respondent argues that Complainant's contention that Respondent should have asked for Complainant's permission is misplaced as "[t]here is no requirement under the Policy or adjacent trademark law for a registrant to seek a license or 'permission' before registering a domain for a legitimate, non-confusing educational purpose".

6. Discussion and Findings

Under paragraph 4(a) of the Policy, to succeed Complainant must satisfy the Panel that:

(i) the disputed domain name is identical or confusingly similar to a trademark or service mark in which Complainant has rights;

(ii) Respondent has no rights or legitimate interests in respect of the disputed domain name; and

(iii) the disputed domain name was registered and is being used in bad faith.

A. Identical or Confusingly Similar

Ownership of a trademark registration is generally sufficient evidence that a complainant has the requisite rights in a mark for purposes of paragraph 4(a)(i) of the Policy. WIPO Overview of WIPO Panel Views on Select UDRP Questions ("WIPO Overview 3.1") at section 1.7. Complainant has provided evidence that it owns a trademark registration for the EQUIFAX mark.

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. *Id.*

Here, the disputed domain fully incorporates the EQUIFAX mark. Although the addition of a hyphen and the common word "credit" at the tail of the disputed domain name may bear on the assessment of the second and third elements, the Panel finds the addition of such elements does not prevent a finding of confusing similarity between the disputed domain name and the EQUIFAX mark for purposes of the Policy WIPO Overview 3.1, section 1.8.

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

B. Rights or Legitimate Interests

Paragraph 4(c) of the Policy provides a list of circumstances in which a respondent may demonstrate rights or legitimate interests in a disputed domain name.

Here, the Panel is faced with the somewhat unique situation where Respondent is using the disputed domain name that is based on Complainant's EQUIFAX mark in connection with simulated phishing attacks on employees of Respondent's corporate clients in a context where (i) there is no website or content hosted at the disputed domain name, (ii) Respondent posits that it has taken precautionary steps to avoid commercial

harm to Complainant, and (ii) anyone involved in Respondent's training program who clicks on the domain name link is provided immediate feedback that they have responded to a simulated phishing attack.

Respondent contends that this is a legitimate non-commercial fair use given that the use of the disputed domain name is only in connection with Respondent's legitimate educational computer security training programs for its corporate clients, is not meant to mislead consumers for commercial gain, is being done in a controlled environment involving only employees of its customers, and is being done with clear precautionary steps to prevent access to the disputed domain name by consumers generally.

Complainant counters that Respondent's use of the disputed domain name is not a legitimate fair use nor a bona fide use as Respondent is using the disputed domain name as part of its for profit services, has done so without permission from Complainant, is impersonating Complainant for Respondent's profit, and is causing potential harm to Complainant by associating Complainant with phishing or spam in the minds of those consumers who do not click on links associated with the disputed domain name.

The primary issue before the Panel is whether Respondent's use of the disputed domain name as noted above constitutes 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" under Paragraph 4(c)(iii) of the Policy. To be sure, Respondent's actions here, on an initial view, do not fall squarely within the parameters of Paragraph 4(c)(iii) given that Respondent is not diverting consumers per se for commercial gain or to tarnish Complainant's mark and is using the disputed domain name within a controlled environment as part of a bona fide security awareness educational program. However, the concept of fair use and what constitutes such has evolved with over 25 years of UDRP jurisprudence to include broader considerations of such things as impersonation, commercial gain and the like.[1]

Notably, two panels that have considered UDRP complaints involving Respondent under similar circumstances have come to different conclusions. In August 2021, the Panel in *Aetna v. Knowbe4*, while not ruling on whether Respondent was making a bona fide use or legitimate interest, acknowledged that the matter was a close call and found that Complainant had not established that Respondent's registration and use of a domain name based on the AETNA mark for simulated phishing attacks was being done to take unfair advantage of or otherwise intentionally abuse or tarnish the AETNA mark. The panel further noted that Respondent's use of the domain name at issue as part of its security awareness services did not appear to be the sort of wrong covered by the Policy, but rather was an issue that possibly fell outside the scope of the Policy for which the courts were better suited to handle. By contrast, in *Home Depot v. Knowbe4*, a decision that issued nine months later, the panel found that Respondent's use of the domain name based on the HOME DEPOT mark for simulated phishing attacks as part of it security awareness programs was not a legitimate use as Respondent did not own that mark and had appropriated and used the mark without Complainant's permission as part of its for-profit business.

While on their face these two decisions seem irreconcilable, on closer examination these decisions do not necessarily require the Panel to take an "either or" approach in the matter. The panel in *Home Depot v. Knowbe4,* clearly found on the facts presented in that matter that Respondent lacked a legitimate interest, noting as follows: "It is clear that Respondent is not using the Domain Name in connection with a genuine phishing program, or for a website which impersonates or competes with Complainant or otherwise trades on Complainant's reputation and goodwill. The Panel also recognizes that Respondent is taking precautions to ensure that the Domain Name is used only in a controlled testing environment and that its primary focus is on training and education in an important field-cyber security. None of this, however, addresses the underlying fact that Respondent does not own the HOME DEPOT mark, and that it appropriated and is using that mark without Complainant's permission as part of its for-profit business".

---

[1] An example of such can be found in the context of bona fide noncommercial criticism. Some Panels have approached whether a use of domain name constitutes a fair use, even when used for genuine noncommercial website, by applying an impersonation test. See, e.g., *Dover Downs Gaming & Entertainment, Inc. v. Domains By Proxy, LLC / Harold Carter Jr, Purlin Pal LLC*, WIPO Case No. D2019-0633. See also WIPO Overview 3.1 at sections 2.4 through 2.6.

In the limited discussion of whether Respondent had a legitimate interest in the disputed domain name in *Aetna v. Knowbe4* decision, the panel noted on the facts presented in that case some of this similar concerns as follows without ruling on the legitimacy of Respondent's actions: "The Panel observes, on the one hand, that even if the Domain Name is being used for alleged educational purposes, the Domain Name itself (encompassing Complainant's mark) still may tend to suggest sponsorship or endorsement by Complainant, even if as the Domain Name is used only in the context of Respondent's educational training programs. On the other hand, the Domain Name is not connected to any website (public or otherwise), so its use (as noted in Respondent's precautionary steps) is uniquely limited and not a type of use that seeks to use Complainant's trademark for any kind of commercial leverage or benefit".

To this Panel, the issue raised by these two decisions, and the facts presented in this proceeding, turns on whether Respondent is in fact using the disputed domain name that incorporates the EQUIFAX mark for commercial gain. See, e.g., WIPO Overview 3.1 at Sections 2.5.1 through 2.5.3.

To begin, it is obvious that Respondent is not using the disputed domain name in the traditional sense to mislead consumers, such as by redirecting them to a website, for commercial gain. To the Panel, there is no issue that Respondent's educational security awareness programs which addresses cybersecurity concerns is a legitimate business even as a for-profit concern. The question then is whether Respondent by using the well-known mark of another in a domain name as part of its educational program to simulate phishing attacks on employees of its customers is going beyond a fair use and falling into the sphere of using such a domain name for commercial gain.

To be sure, there is no per se need by Respondent to conduct simulated phishing attacks by registering and using domain names based on the well-known marks of others without authorization for purposes of training or educating employees on security awareness. Respondent does not argue otherwise, but asserts that it does so from time to time for purposes of allowing its corporate customers "to perform simulated social engineering exercises". And while such a simulated phishing attack may be an effective training tool, a contention Complainant contests, it does not appear to be the only way to train employees about cybersecurity (and Respondent does not contend otherwise).

The Panel, to be clear, makes no finding on the effectiveness of simulated phishing attacks. That being said, given that Respondent appears to contend that use of the disputed domain name is a necessary tool for its security awareness programs, there is a question as to whether such is in fact necessary. In the Panel's view, Respondent's use of a domain name based on a known trademark is not as necessary as say having an actual physical branded car engine in order to train a mechanic on how to repair that branded engine. Respondent could use a multitude of other domain names to effectuate its simulated phishing schemes or could use other potentially effective techniques to teach security awareness.

The question the foregoing thus raises is why Respondent needs to use domain names based on well-known marks for its simulated phishing attacks. To the Panel, the answer to that question appears to relate to Respondent 's ability to sell its services to its customers. Using domain names that are based on known marks are likely more effective and may have a greater percentage chance of misleading unsuspecting employees into clicking on the links associated with the domain name than domain names that are not based on known marks or which include fictitious brands. As there is a likely higher response rate from domain names based on known marks, Respondent, as a for profit company, can then promote the effectiveness of its simulated phishing attacks as a training tool when it sells such to its corporate clients.

Using domain names based on fictitious names or marks or lesser-known brands likely elicit a lower response rate from unsuspecting employees as they are less likely to be clicked on than something that is more clearly known or recognized. Such lower response rate might affect the effectiveness of Respondent's simulated phishing attacks which could then impact on the value of such services to potential customers as a training tool. Put another way, Respondent has a clear commercial interest in selling its training programs and platform by emphasizing the effectiveness of its simulated phishing attacks.

Here, the disputed domain name includes the EQUIFAX mark with the term "credit" which is a term that appears to be associated with services offered by Complainant (particularly as some consumers monitor their own credit rating using Complainant's services (see "www.equifax.com")). The disputed domain name is thus more likely to elicit a response from a simulated phishing attack, given that it is more likely to be seen as connected to Complainant and its services, by implying a high degree of association if not crossing the line towards impersonation of Complainant. This makes the disputed domain name more valuable to the Respondent in the Panel's view.

This is particularly telling in view of the prior decisions in *Aetna v. Knowbe4* and *Home Depot v. Knowbe4* that likewise involved domain names based on known marks. There is no evidence before the Panel that Respondent in fact uses for its simulated phishing attacks anything other than domain names that are based on the well-known marks of others or which are readily known to consumers. It thus appears that Respondent's model is to essentially impersonate known brands to make the for-profit services it provides more effective. Such targeting of well-known brands without any authorization to imply an affiliation for purposes of rendering Respondent's simulated phishing attack services more effective, and to thus profit from selling such services to others, is a commercial use for the benefit of Respondent and is not a fair use. The fact that Respondent is operating a legitimate business, one that is educational in nature, simply does not make Respondent's actions in targeting a well-known brand without authorization to enhance and make its services more valuable as being a legitimate noncommercial fair use. See, e.g., WIPO Overview 3.1, 2.5.3.

The Panel thus finds the second element of the Policy has been established.

C. Registered and Used in Bad Faith

Respondent's conduct as discussed in the rights or legitimate interests analysis above also supports a finding of bad faith registration and use. While Respondent's actions do not fall within any of the circumstances articulated in Paragraph 4(b) of the Policy, Paragraph 4(b) recognizes that bad faith conduct can appear in many different ways and thus adopts a non-exclusive approach to bad faith, listing some examples without attempting to enumerate all of the possible versions. See, e.g., *Worldcom Exchange, Inc. v. Wei.com, Inc.*, WIPO Case No. D2004-0955.

Here, there is no dispute that Respondent was clearly aware of Complainant's EQUIFAX mark when it registered and began using the disputed domain name. Respondent may have believed that it did not need to obtain permission from Complainant to use the EQUIFAX mark, but clearly it knew that it did not have permission to do so and never sought such (perhaps on account of the reactions it had faced previously from at least one other brand owner. See *Aetna v. Knowbe4*.)

The fact that Respondent appears to be using domain names based on the known marks of others as opposed to fictitious brands supports the notion that Respondent is targeting known brands, such as the EQUIFAX mark of Complainant, to render its simulated phishing attacks more effective. As already noted above, such use is, in and of itself, a commercial use for the benefit of Respondent, as the simulated phishing services based on Complainant's well-known trademark are more likely to aid Respondent's ability to sell its services to corporate customers. To be sure, Respondent was well aware that its registration and use of the disputed domain name was concerning to some brand owners and perhaps crossed the line in light of the *Home Depot v. Knowbe4* decision and the ambivalent language of the prior *Aetna v. Knowbe4* decision. Respondent, however, plowed ahead at its own risk (instead of e.g., simply relinquishing the disputed domain name, it undertook the time and expense of engaging legal counsel) and thus cannot be said to have proceeded innocently in the belief that its use of domain names impersonating or carrying a high degree of implied affiliation constituted a fair use.

In all, while the Panel is of the view that this case presents a nuanced issue under the Policy, Respondent's registration and use of the disputed domain name to make its simulated phishing attacks more effective, for its ultimate financial benefit, is an attempt to take advantage of the known mark of another for the benefit of Respondent as contemplated under Paragraph 4(b) of the Policy.

The Panel thus finds the third element of the Policy has been established.

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 <equifax-credit.com> be transferred to Complainant.

/Georges Nahitchevansky/
Georges Nahitchevansky
Presiding Panelist

/Robert A. Badgley/
Robert A. Badgley
Panelist

/Christopher S. Gibson/
Christopher S. Gibson
Panelist (Concurring)

Date: May 15, 2026

Concurring Opinion of Christopher S. Gibson

I write separately to concur in this decision because I served as Presiding Panelist in *Aetna Inc. v. On behalf of help-aetna.com owner / Whois Privacy Service / Manager / KnowBe4,* WIPO Case No. D2021-1565. As noted in that decision, the case presented a close call under the Policy, as does this one; it was a case where the panel made no ruling on whether Respondent had established rights or legitimate interests in the disputed domain name; and acknowledged that the case might be better suited for the courts. Upon further reflection, and in light of the fuller record and arguments presented in this case, and the subsequent decision in *Home Depot Product Authority v. Domain Owner / Knowbe4*, Forum Claim No. 1990823 (May 25, 2022), where the same Respondent registered a domain name incorporating the well-known HOME DEPOT trademark, I now join the majority's decision here.

In particular, I agree that the disputed domain name used by Respondent impersonates or at least carries a high degree of implied affiliation with Complainant for Respondent's own commercial benefit. Respondent's use creates a risk of confusion, reputational harm, and association of Complainant with phishing or spam activity, while at the same time leveraging Complainant's well-known EQUIFAX mark to enhance the attractiveness of Respondent's for-profit simulated security-awareness services.

The record further supports the conclusion that Respondent's business model likely benefits from the registration and use of domain names incorporating the well-known marks of others in order to increase the realism, and therefore the commercial value, of its training services. Notably, there is no evidence before the Panel that Respondent employs fictitious brands, generic terminology, or other non-infringing alternatives for these simulated phishing campaigns. Rather, Respondent appears to rely specifically upon the recognition associated with famous third-party marks. I agree with the Panel that there is no per se need by Respondent to conduct security awareness simulations by using domain names based on the well-known marks of others without their authorization.

Finally, I observe that Respondent's approach creates a broader concern under the Policy. There appears to be no principled limiting point as to the number of domain names corresponding to well-known marks that Respondent – or similar copycat security-awareness companies – could register and use in order to promote their for-profit security training services. Such a model risks normalizing the widespread registration of third-party trademarks in impersonating domain names under the guise of "training" and "awareness" activities, while shifting the resulting confusion and reputational harms onto the mark owners and the public.

/Christopher S. Gibson/
Christopher S. Gibson
Panelist (Concurring)
Date: May 15, 2026