



CANADIAN INTERNATIONAL INTERNET DISPUTE RESOLUTION CENTRE

DOMAIN NAME DISPUTE

ADMINISTRATIVE PANEL

DECISION

CIIDRC case number:	17134-UDRP	Decision date: February 27, 2022
Domain Name:	northssave.com	
Panel:	Zak Muscovitch	
Complainant:	Northern Savings Credit Union	
Complainant's representative:	Kristél Kriel of MLT Aikins LLP	
Respondent:	Jennifer Lewis	

1. PROCEDURAL HISTORY

On January 27, 2022, the Complainant submitted a Complaint (the "Complaint") to the Canadian International Internet Dispute Resolution Centre ("CIIDRC") pursuant to the Internet Corporation for Assigned Names and Numbers ("ICANN") Uniform Dispute Resolution Policy ("UDRP" or the "Policy") and in accordance with the UDRP Rules and CIIDRC Supplementary Rules (collectively, the "UDRP Rules and Supplemental Rules").

On January 27, 2022 the CIIDRC notified Wild West Domains, LLC, the registrar (the "Registrar") of the disputed domain name, northssave.com (the "Domain Name") that the Complaint had been filed with the CIIDRC in respect of the Domain Name and requested that the Registrar lock the Domain Name in accordance with UDRP Rule 4(b) and to provide the full Registration Data for the Domain Name in accordance with Appendix E to ICANN's

Temporary Specification for gTLD Registration Data, effective May 25, 2018 (the “Registration Data”).

On February 3, 2022, the Registrar confirmed that it had locked the Domain Name and provided the Registration Data in respect of the Domain Name, namely the Whois information.

On February 3, 2022, following the CIIDRC’s confirmation of the Complaint’s administrative compliance with the Policy in accordance with UDRP Rule 4(b), the CIIDRC notified the Respondent, Jennifer Lewis (the “Respondent”) of this administrative proceeding pursuant to CIIDRC Supplementary Rule 5(b) and forwarded the Notice of Commencement of the UDRP proceeding along with the Complaint, to the Respondent in accordance with the Respondent’s contact details as provided by the Registrar in the Registration Data. Delivery of the Complaint was effected by email and by ExpressPost. Confirmation of delivery by ExpressPost was received.

No Response was filed by the due date of February 23, 2022. On February 24, 2022, the Respondent was notified by email in accordance with the Registration Data, that the due date for filing the Response had expired and that therefore, pursuant to UDRP Rule 5(f), a Panel would decide the dispute based upon the Complaint, absent exceptional circumstances.

On February 25, 2022, pursuant to the Complainant’s election to have this dispute decided by a single-member Administrative Panel, the undersigned was appointed by the CIIDRC as a single-member Panel (the “Panelist”) in accordance with the UDRP Rules and CIIDRC Supplemental Rules. The Panelist duly completed and returned to the CIIDRC, a Statement of Acceptance and Declaration of Impartiality and Independence, dated February 27, 2022.

Having examined the record, the Panelist finds that the CIIDRC has discharged its responsibilities under Paragraph 2(a) of the UDRP Rules “to employ reasonably available means calculated to achieve actual notice to Respondent”.

The Panelist further finds that the Domain Name is subject to the Policy pursuant to the Registrar’s Registration Agreement, which incorporates the Policy by reference at Section 6.

2. RELIEF SOUGHT

The Complainant request that the Domain Name be transferred from Respondent to Complainant pursuant to Paragraph 4(i) of the Policy.

3. FACTS ALLEGED BY THE PARTIES

The Complainant, Northern Savings Credit Union, states that it is a community-based and member-owned credit union that has been operating in Canada since 1940 providing financial services to more than 14,000 individuals and businesses in Prince Rupert, Terrace, and Haida Gwaii, British Columbia, Canada. The Complainant states that it registered its domain name, northsave.com, in 1996 and uses it for its website.

The Complainant is the registrant of the trademark, WWW.NORTHSAVE.COM, which was registered with the Canadian Intellectual Property Office (“CIPO”) on August 27, 2002, as CIPO Registration No. TMA566428, in connection with *inter alia*, credit union services, online financial services information, and Internet financial transaction services.

The Complainant alleges that the disputed Domain Name is nearly identical to the Complainant’s NorthSave.com domain name used for the Complainant’s website, except for a one-letter difference (an additional ‘s’), and is clearly designed to be confusingly similar in order to deceive.

The Complainant alleges that the disputed Domain Name is a “lookalike” domain name which has been used to send fraudulent phishing emails to the Complainant’s employees, members, stakeholders and others since the Domain Name was registered by the Respondent on January 6, 2022. The Complainant alleges that the disputed Domain Name was created on the same day as the Respondent began sending out “phishing” emails using the disputed Domain Name to deceive recipients.

The Complainant provides three examples of “phishing” emails which it states have impersonated the Complainant’s staff in an attempt to trick recipients into clicking on a fraudulent link and to enter the recipient’s own credentials. The Complainant alleges that the

phishing emails are designed to appear as though they require urgent participation from the recipient in a competitive bidding process related to a “Request for Proposal” or “RFP”. For example, one email appears to be sent by the Complainant’s “Vice-President of Finance”, with an email address @northssave.com (note the additional letter ‘s’), inviting the recipient to urgently submit a proposal in accordance with the RFP. The email includes a link to a Microsoft “SharePoint” document and provides a deadline for the recipient to respond to the RFP. Ostensibly, when a recipient clicks on the link, they are asked to provide their credentials which could then be used for further fraudulent purposes, or by clicking the included link, the recipient’s computer could possibly be infected with malicious code designed to later obtain further confidential information from the recipient.

Upon becoming aware of the fraudulent emails impersonating the Complainant, the Complainant immediately took certain steps including retaining forensic experts and external legal counsel to investigate, contain, and address the situation. The Complainant also requested that the Domain Name’s Registrar “lock” the Disputed Domain Name to prevent further harm to the Complainant and to others, apparently without success.

The Complainant states that given that the disputed Domain Name is being used as part of an ongoing “cyber attack” impacting the public, it is “critical that the disputed Domain Name be locked as soon as possible to minimize future harm to the Complainant and others”.

As aforementioned, the Respondent did not respond to the Complaint.

4. CONTENTIONS OF THE PARTIES

The Complainant submits that the disputed Domain Name, northssave.com, is nearly identical to its northsave.com domain name (with an additional letter ‘s’ inserted) and that it is clearly designed to be confusingly similar to the Complainant’s genuine domain name in order to deceive.

The Complainant also alleges that the Respondent has no rights or legitimate interest in the disputed Domain Name because the Domain Name was immediately upon its registration,

used for fraudulent phishing emails. The Complainant alleges that there can be no rights or legitimate interest where a domain name is used for illegal activity.

The Complainant also alleges that the Domain Name was registered and used in bad faith. The Complainant states that the fact that the Domain Name was registered and was immediately put to unlawful use in a phishing scheme is clear evidence that the Disputed Domain Name was registered and is being used in bad faith. The Complainant alleges that targeting a trademark for fraudulent use is exactly the type of conduct that the UDRP is meant to address.

As aforementioned, the Respondent did not respond to the Complaint.

5. DISCUSSION AND FINDINGS

5.1 Requirements

Paragraph 4(a) of the Policy sets forth a three-part test to determine whether a transfer is justified and requires that “the complainant must prove that each of [the] three elements are present.” The three-part test is as follows:

1. That the Domain Name is identical or confusingly similar to a trademark or service mark in which the Complainant has rights;
2. That the Registrant has no rights or legitimate interests in the Domain Name; and
3. That the Domain Name has been registered and being used in bad faith.

Even in cases where no Response is delivered, panels must evaluate the allegations and the evidence presented by the complainant to determine whether the complainant has proven each of the Policy’s three elements. The Panelist will consider each of these requirements in turn.

5.2 Analysis

5.2.1 That the Domain Name is Identical or Confusingly Similar to a Mark in which the Complainant has Rights

The Complainant is the registrant of the Canadian registered trademark, WWW.NORTHSAVE.COM, registered August 27, 2002. The Complainant's trademark disclaims the right to the exclusive use of the letters "WWW" and ".COM" apart from the trademark, which is consistent with the fact that these elements are non-distinctive and merely refer to the "World Wide Web" and the .com top-level domain. The predominant and distinctive element of the trademark is clearly NORTHSAVE, and it is that element which must be compared to the disputed Domain Name. Moreover, and though not specifically referenced by the Complainant, the Complainant is also the registrant of CIPO Trademark Registration No. TMA1081159 for NORTHSAVE alone, registered August 19, 2020 in connection with various goods and services, including but not limited to credit union and related services. Although not necessary, given that the Complainant also has WWW.NORTHSAVE.COM, this trademark can also be compared with the Domain Name.

When comparing a domain name to a trademark for the purposes of the determining whether the domain name is identical or confusingly similar to a complainant's trademark, the .COM element within a domain name is usually disregarded (*See for example, [Eastman Chemical Company v. Kumar Patel](#)* Forum Claim Number: FA0507000524752 (Sept. 7, 2005). However in this particular case, the Complainant's trademark actually includes the .COM element and therefore perhaps the .COM element of the Domain Name need not be disregarded. Regardless, when comparing the predominant and distinctive portion of the Complainant's WWW.NORTHSAVE.COM trademark with the Domain Name, even when disregarding the .COM element within the Domain Name, it is clear that the Domain Name is nearly identical and certainly confusingly similar, as the only difference is the inclusion of an additional letter, "s", within NORTHSAVE. Likewise, the Domain Name is nearly identical and certainly confusingly similar to the Complainant's NORTHSAVE trademark for the same reason.

As held in *[Cenovus Energy Inc. v. McKenzie](#)*, CIIDRC Case No. 15633-UDRP (July 15, 2021), adding a letter into a complainant's mark and including a gTLD will not negate confusing similarity. Accordingly, the Panel finds that the Domain Name is confusingly similar to Complainant's trademarks in satisfaction of paragraph 4(a)(i) of the Policy.

4.2.2 That the Respondent has No Rights or Legitimate Interest in the Domain Name

As the Complainant contends, it is now well established that the Complainant must first make a *prima facie* case that the Respondent lacks rights and legitimate interests in the disputed domain name and then the burden shifts to the Respondent to show that it does in fact have rights or legitimate interest in the domain name.

The Panel finds that the Complainant has made out a *prima facie* case. The Respondent purposefully selected and registered the Domain Name because it corresponds to the Complainant's trademarks, with the sole difference being the inclusion of an additional letter "s" which was intentionally included to deceive. The Respondent selected the Domain Name for a phishing scheme targeting a financial institution specifically because the Domain Name looked very similar to the Complainant's trademarks and to the Complainant's genuine domain name, thereby hoping that recipients of the phishing email would not notice the small difference in the Domain Name and thereby be deceived into providing credentials and/or confidential information to the Respondent. It is well established that a fraudulent phishing scheme involving a purposefully confusingly similar domain name cannot give rise to rights or a legitimate interest by a registrant (See for example, [*Whitehall Specialties, Inc. v. Registration Private et al.*](#), WIPO Case No. D2021-0716 (May 20, 2021), wherein the Panel stated the use of a confusingly similar, deceptive domain name for an email scam has previously been found by panels to be sufficient to establish that a domain name has been registered and is being used in bad faith).

A comparable situation arose in [*Sunova Credit Union v. Wimbush*](#), CIIDRC Case No. 13036-UDRP, cited by the Complainant, wherein no rights or legitimate interest were found because the Respondent targeted the complainant and its trademark to impersonate the complainant and carry out fraudulent activities with a direct impact on the members doing business with the complainant and on the complainant itself. In that case the Panel confirmed that using a domain name for illegal activity can never confer rights or legitimate interests on a respondent.

The Respondent did not respond to the Complaint and in particular has not rebutted the *prima facie* case made out by the Complainant. Moreover, based upon the facts and evidence provided by the Complainant in the record, the Panel finds that the Respondent has no rights or legitimate interest in the Domain Name because registration and use of the Domain Name

selected to deceive for the purpose of engaging in a phishing scam cannot confer any rights or legitimate interest upon the Respondent.

4.2.3 That the Respondent has Registered and Used the Domain Name in Bad Faith

To establish bad faith for the purposes of the Policy, the Complainant must show that the disputed domain name was registered in bad faith and that it has been used in bad faith. Paragraph 4(b)(ii) of the Policy states bad faith may be found where the Respondent uses the Domain Name to intentionally attempt to attract, for commercial gain, Internet users to a web site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your web site or location or of a product or service on your web site or location. That is the case here. Also, as the Panelist stated in [*Cenovus Energy Inc. v. McKenzie*](#), *supra*, the criteria set out in Policy Paragraph 4(b) for establishing bad faith are not exhaustive. Rather, complainants in UDRP proceedings may also rely on conduct that is bad faith within the generally accepted meaning of that expression even if the particular indicia of bad faith is not specifically enumerated in the Policy. The Respondent's fraudulent phishing scam clearly constitutes such non-enumerated grounds for finding bad faith registration and use.

It is obviously not a coincidence that the Respondent selected a Domain Name that corresponds nearly identically to the Complainant's trademarks and by extension, to the Complainant's website and associated email addresses. The Complainant obviously purposefully registered the Domain Name in bad faith to capitalize upon the deception that the Domain Name would facilitate. The Respondent obviously used the Domain Name in bad faith when sending out phishing emails to the Complainant's members and to others, in an attempt to obtain credentials and possibly other confidential personal data from the unwitting recipients who clicked on the embedded links.

The Panelist therefore finds that the Respondent was certainly aware of the Complainant and specifically targeted the Complainant's trademarks when registering and using the disputed Domain Name in an unlawful manner. This is a very serious instance of abusive domain name registration, as financial institutions in particular, cannot tolerate any form of fraud or abuse particularly when the fraud is intentionally misrepresented as emanating from the Complainant

itself. As noted by the Panelist in [Sunova Credit Union v. Wimbush](#), *supra*, this practice falls squarely within the type of conduct that the UDRP is meant to address and accordingly the Panelist finds that the Domain Name was registered and used in bad faith.

The Panelist also notes that in such cases of serious and potentially ongoing fraudulent activity by a Respondent in clear contravention of the Policy, it is incumbent upon the Dispute Resolution Provider and the Panelist to act as quickly as reasonably possible to provide the requested remedy to the Complainant, particularly where other steps to stem the fraudulent activity have failed. The Panelist is pleased that this has been done in this case.

4 DECISION and ORDER

For the above reasons, and in accordance with Paragraph 4 of the Policy, Paragraph 15 of the UDRP Rules, and Rule 10 of the CIIDRC Supplemental Rules, the Panel orders that the Domain Name, northssave.com, be transferred to the Complainant.

Made as of February 27, 2022

SIGNATURE OF PANEL



Zak Muscovitch

