



September 23, 2020

Ryan Johnson, Chief Technology Officer
Rocklin USD
2615 Sierra Meadows Drive
Rocklin, CA 95677

Dear Mr. Johnson,

As you know, last Thursday, September 17, 2020, Nutri-Link Technologies Inc. discovered a vulnerability on our website <https://admin.nlappscloud.com/statuslookup/SelectDistrict>. The vulnerability would have allowed a person visiting the site to bypass our authentication requirements and view information stored in our database. In particular, a person could view the full name, student ID number, grade level, free or reduced lunch eligibility status, and the lunch application confirmation number of any student in the Rocklin USD, whose information is on our site.

Upon becoming aware of the situation, we immediately removed the vulnerability from our site. At this time, we believe it was present on the site for a short period of time and was discovered by very few people (none of whom were acting with ill intent). We have no reason to believe that any malicious actor accessed information on the site during the period of compromise, and we have no reason to believe there is any risk to the data stored in the site.

While we continue to investigate the situation we, in an abundance of caution and in a desire to maintain transparency, wanted to make you aware of it right away. We value the trust you place in us and take our responsibility to safeguard your students' personal information seriously. We will update you of any significant developments in our investigation.

We apologize for any inconvenience or concern this incident might cause and invite you to reach out to us with questions at 404-437-7964 from 8 a.m. to 5 p.m. Eastern, Monday through Friday.

Sincerely,

A handwritten signature in black ink that reads "Michael Lobato". The signature is written in a cursive, flowing style.

Michael Lobato, President
Nutri-Link Technologies, Inc.