

Jena Valdeteo
Tel 312.456.1025
valdeteroj@gtlaw.com

April 22, 2021

Attorney General

Office of the Attorney General
33 Capitol Street
Concord, NH 03302

attorneygeneral@doj.nh.gov

Dear Sir or Madam:

We are writing to inform you that our client, Veada Industries, Inc. ("Vaeda") is notifying approximately 8 individuals who reside in New Hampshire of a data security incident that may have impacted some of their personal information.

We discovered on March 23, 2021 that the veada.com website was infected with malware which could have exposed customer information to an unknown third party. While we have no evidence that the attackers actually acquired any personal information, the third party potentially had access to data for customers on veada.com who made purchases between November 1, 2019 and March 23, 2021. Veada took immediate action to prevent further unauthorized access and to secure its website. Veada commenced an investigation to determine how the incident occurred and what information, if any, was impacted. As a result of its investigation, Veada determined that it is possible that an unauthorized third party may have obtained access to the following personal information:

[REDACTED]
to make purchases on the website.

Veada has taken steps to prevent a reoccurrence - taking the site permanently offline, improving security controls, and evaluating policies and procedures related to information security. We have also notified law enforcement.

Veada has or will mail notifications to all potentially affected individuals on April 23, 2021. An example of the notification is attached.

Please contact me for any additional information.

Sincerely,



Jena M. Valdeteo

Shareholder

Greenberg Traurig, LLP | Attorneys at Law
77 West Wacker Drive | Suite 3100 | Chicago, Illinois 60601 | T +1 312.456.8400 | F +1 312.456.8435
Albany. Amsterdam. Atlanta. Austin. Berlin. Boston. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Houston. Las Vegas. London. Los Angeles.
Mexico City. Miami. Milan. Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Sacramento. Salt Lake
City. San Francisco. Seoul. Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv. Tokyo. Warsaw. Washington, D.C. West Palm Beach. Westchester
County.

Operates as: ~Greenberg Traurig Germany, LLP; *A separate UK registered legal entity; +Greenberg Traurig, S.C.; »Greenberg Traurig
Santa Maria; ∞Greenberg Traurig LLP Foreign Legal Consultant Office; ^A branch of Greenberg Traurig, P.A., Florida, USA; ⓂGT Tokyo
Horitsu Jimusho and Greenberg Traurig Gaikokuhojimbegoshi Jimusho; ~Greenberg Traurig Grzesiak sp.k.

www.gtlaw.com



[Mail Address]
[Mail Address 2]
[Mail Address 3]

<<Name >>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>> <<Date>>
<<Country>>

Dear <<Name>>:

Notice of Data Breach

What Happened?

We discovered on March 23, 2021 that the veada.com website was infected with malware which could have exposed your customer information to an unknown third party. Upon discovering the attack, we took immediate action to stop any further access and investigated the incident.

What Information was Involved?

While we have no evidence that the attackers actually acquired any personal information, the third party potentially had access to data for customers on veada.com who made purchases between November 1, 2019 and March 23, 2021. This would include names, addresses, payment details, including the payment card number, CVV code and expiration date, for the card you used to make a purchase on the website.

What We are Doing

We take the security of personal information very seriously, and we want to assure you that we've already taken appropriate steps to prevent a reoccurrence – taking the site permanently offline, improving security controls, and evaluating policies and procedures related to information security. We have reported this incident to our payment processor and appropriate law enforcement.

What You Can Do

We recommend that you review your payment card account statements for any unauthorized transactions and report any unauthorized activity to the bank that issued your card immediately. You are not responsible for unauthorized charges on your credit card in an amount over \$50 if you report the charges promptly within the adequate timeframe under the Fair Credit Billing Act, although most card issuers do not seek to recover fraudulent charges from cardholders. Please also review the enclosed "Additional Important Information" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (FTC) regarding details on how to place a fraud alert or a security freeze on your credit file, should you choose to do so. You can also contact the FTC for more information.

For More Information

If you have additional questions or concerns regarding this incident, please call 1-(855) 484-1185 between 8 am and 5:30 pm, Central Time, Monday through Friday excluding major U.S. holidays.

We take the security of all information in our systems seriously. Please know that the protection of your personal information is our utmost priority, and we sincerely regret any inconvenience that this matter may cause you.

Sincerely,

Veada Industries, Inc.

Additional Important Information

For residents of Iowa: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident, and that you have rights pursuant to the federal Fair Credit Reporting Act. Please see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island:

You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

DC Attorney General	Maryland Office of Attorney General	Rhode Island Office of Attorney General	North Carolina Attorney General	New York Attorney General
400 6th Street NW Washington, D.C. 20001 1-202-727-3400 www.oag.dc.gov	200 St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us	150 South Main Street Providence RI 02903 1-401-274-4400 www.riag.ri.gov	9001 Mail Service Ctr Raleigh, NC 27699 1-877-566-7226 www.ncdoj.com	120 Broadway 3rd Floor New York, NY 10271 www.ag.ny.gov

Federal Trade Commission, Consumer Response Center

600 Pennsylvania Ave, NW Washington, DC 20580

1-877-IDTHEFT (438-4338) www.identitytheft.gov

For residents of Massachusetts and Rhode Island: You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states: Although payment card numbers cannot be used to obtain credit in your name, the law requires that we provide you with the following information. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your free credit reports for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (<https://www.experian.com/fraud/center.html>), or Transunion (<https://www.transunion.com/fraud-victim-resource/place-fraud-alert>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze for yourself or your spouse or a minor under 16: (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
www.experian.com
888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016-0200
www.transunion.com
800-680-7289

This notification was not delayed by law enforcement notification.