



Legal Counsel.

Kurt R. Hunt
DINSMORE & SHOHL LLP
(513) 977-8101 (direct) · (513) 977-8141
(fax)
kurt.hunt@dinsmore.com

May 22, 2020

VIA E-MAIL (DOJ-CPB@DOJ.NH.GOV) AND U.S. MAIL

Attorney General Gordon J. MacDonald
New Hampshire Department of Justice
Attn: Data Security Breach
33 Capitol Street
Concord, NH 03301

Re: Notification of Data Security Incident- Volk Optical Inc.

Dear Mr. MacDonald:

My office represents Volk Optical Inc. (“Volk”) in connection with an incident that involved the possible compromise of personal information of some of its customers including, notably, one (1) New Hampshire resident. We provide this notice on behalf of Volk pursuant to N.H. Rev. Stat. §359-C:20.

This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While Volk is notifying you of this incident, Volk does not waive any rights or defenses relating to the incident or this notice, or the applicability of New Hampshire law on personal jurisdiction.

Nature of the Security Breach or Unauthorized Use or Access

Volk contracts with a PCI-compliant third party hosting service to allow Volk to make volk.com (the “Volk Website”) available to its customers and visitors generally. On May 1, 2020, Volk began investigating the website’s functionality after learning of the possible compromise of a payment card recently used on the Volk Website. The investigation revealed on May 14, 2020 that a malicious script had been installed on the web server hosting the Volk Website granting a malicious third party with remote access to the server. As a result, an unknown third party may have had unauthorized access to personal information submitted in connection with a transaction on the Volk Website between February 11, 2020 and May 8, 2020. Specifically, the following information provided during a transaction was potentially accessible: credit card data including name, billing address, credit card number, credit card expiration date, and CCV number.

Number of New Hampshire Residents Affected

The incident may have impacted one (1) New Hampshire resident. Volk will be notifying this individual on May 26, 2020 pursuant to N.H. Rev. Stat. §359-C:20. Enclosed is a sample of the notice that will be sent to the potentially impacted individual.

Steps Taken Relating to the Incident

Upon learning of the possible compromise, Volk immediately began a forensic investigation utilizing the services of an expert third party forensic team. Even prior to completing the investigation, Volk took the Volk Website off-line to minimize any potential harm. The compromised version of the Volk Website is now permanently offline, and Volk has transitioned its e-commerce activities to a new secure host and platform to keep the compromised web server isolated from Volk's customers going forward. Volk is currently working with its incident response team and privacy legal counsel to identify potential improvements to internal processes and procedures, to help prevent comparable attack in future.

Please do not hesitate to contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Kurt R. Hunt

Dear [INDIVIDUAL NAME]:

I am writing on behalf of Volk Optical Inc. (“Volk”) to inform you of a recent incident that may have exposed some of your personal information.

What Happened

Volk contracts with a PCI-compliant third party hosting service to allow Volk to make volk.com (the “Volk Website”) available to its customers and visitors generally. On May 1, 2020, Volk began investigating the website’s functionality after learning of the possible compromise of a payment card recently used on the Volk Website. The investigation revealed on May 14, 2020 that a malicious script had been installed on the web server hosting the Volk Website granting a malicious third party with remote access to the server. As a result, an unknown third party may have had unauthorized access to personal information submitted in connection with a transaction on the Volk Website between February 11, 2020 and May 8, 2020.

What Information Was Involved

We have found no evidence that your personal information was in fact intercepted or exfiltrated by an unauthorized person. Nevertheless, we are sending you this notice out of an abundance of caution because you made a transaction on the Volk Website during the time period in question. As a result of the malicious script incident, the following information you provided during the transaction was potentially accessible: credit card data including name, billing address, credit card number, credit card expiration date, and CCV number.

What We Are Doing

Upon learning of the possible compromise, Volk immediately began a forensic investigation utilizing the services of an expert third party forensic team. Even prior to completing the investigation, Volk took the Volk Website off-line to minimize any potential harm. The compromised version of the Volk Website is now permanently offline, and Volk has transitioned its e-commerce activities to a new secure host and platform to keep the compromised web server isolated from Volk’s customers going forward. Volk is currently working with its incident response team and privacy legal counsel to identify potential improvements to internal processes and procedures, to help prevent comparable attack in future.

What You Can Do

We highly recommend that you immediately reach out to your payment card provider and obtain a replacement credit card to help prevent fraudulent transactions, and that you review your most recent payment card statements to identify and report any unusual or suspicious charges to your payment card provider.

For More Information

We have worked as quickly as we can to prevent harm to all affected individuals, and we thank you for your understanding. For further information and assistance, please contact Snigdha Katragadda at 440-510-0750 between 9:00 a.m. and 5:00 p.m. US Eastern Standard Time during the business week or email snigdha.katragadda@volk.com.

We thank you for being a loyal customer of Volk Optical. Volk values you as a customer and we respect the privacy of your information and will continue to work closely with our data security and privacy team and legal counsel to ensure we take additional measures to prevent such an attack in the future.

Sincerely,

Snigdha Katragadda
Director, Quality & Compliance

Steps You Can Take to Further Protect Your Information

You can take the following additional steps to protect your information:

- ***Review Your Credit Reports and Notify Law Enforcement of Suspicious Activity***

As a precautionary measure, we recommend that you remain vigilant over the next twelve to twenty-four months by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should immediately report it to the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the “FTC”).

To file a complaint with the FTC, go to <http://www.identitytheft.gov> or call 1-877-ID-THEFT (1-877-438-4338). Complaints filed with the FTC will be added to the FTC’s Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- ***Obtain A Copy of Your Credit Report***

We recommend that you periodically obtain and review a copy of your credit report from each nationwide credit reporting agency, and have any information relating to fraudulent transactions deleted. You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>. You can also elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(800) 685-1111
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
535 Anton Blvd., Suite 100
Costa Mesa, CA 92626

TransUnion
(800) 916-8800
www.transunion.com
P.O. Box 6790
Fullerton, CA 92834

- ***Place A Fraud Alert on Your Credit Report***

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

- ***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 may be able to

use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (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; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, all security freezes are available free of charge. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.)

Additional information is available via the FTC at <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.

- ***Additional Free Resources on Identity Theft***

You may wish to review the tips provided by the FTC on how to avoid identity theft. For more information, please visit <https://www.identitytheft.gov/Info-Lost-or-Stolen> or call 1-877-ID-THEFT (877-438-4338). A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft is available on the FTC's website at <https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf>.