

Colin M. Battersby
Direct Dial: 248-593-2952
E-mail: cbattersby@mcdonaldhopkins.com

October 30, 2019

RECEIVED

NOV 05 2019

CONSUMER PROTECTION

VIA U.S. MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Wolff Shoe Company – Incident Notification

Dear Attorney General MacDonald:

McDonald Hopkins PLC represents Wolff Shoe Company. I am writing to provide notification of an incident at Wolff Shoe Company that may affect the security of personal information of approximately eight (8) New Hampshire residents. Wolff Shoe Company's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Wolff Shoe Company does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Wolff Shoe Company recently experienced suspicious activity on its website. As a result, it immediately contained the issue, engaged external forensic investigators, and commenced a prompt and thorough investigation into the incident. On October 1, 2019, Wolff Shoe Company learned that certain customer credit and debit card information may have been obtained by an unauthorized party when such card information was entered into the payment fields on the website in connection with an online purchase between March 11, 2019 and May 24, 2019. Wolff Shoe concluded that the New Hampshire residents were affected on October 21, 2019.

To date, Wolff Shoe Company does not have evidence demonstrating the unauthorized individuals actually obtained any information and is not aware of any fraudulent transactions at this time. Nevertheless, out of an abundance of caution, Wolff Shoe Company wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Wolff Shoe Company will provide the affected residents with written notification of this incident commencing on or about October 31, 2019 in substantially the same form as the letter attached hereto. Wolff Shoe Company will advise the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents will be advised to remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a

Attorney General Gordon MacDonald
Office of the Attorney General
October 30, 2019
Page 2

regular basis, to call their bank or card issuers if they see any suspicious transactions, and to ask their bank or card issuers whether new cards should be issued. The affected residents will also be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Wolff Shoe Company, protecting the privacy of personal information is a top priority. Since learning of the incident, Wolff Shoe Company has implemented enhanced security safeguards to help protect from similar intrusions. Wolff Shoe Company is also conducting ongoing monitoring of its website and payment portal to ensure that they are secure and cleared of any malicious activity.

Should you have any questions concerning this notification, please contact me at (248) 593-2952 or cbattersby@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,



Colin M. Battersby

Encl.



**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**



Dear 

We wanted to make you aware of a recent data security incident involving potential unauthorized access to payment card data entered at Marmishoes.com, Wolff Shoe Company's online store, over a limited period of time. The privacy and security of your personal information is of utmost importance to us and we are routinely evaluating and improving our security and payment systems to ensure your information is secure.

What Happened?

After suspicious activity on our website was identified, we immediately contained the issue, engaged external forensic investigators, and commenced a prompt and thorough investigation into the incident. As a result of this review, we learned that certain customer credit and debit card information may have been obtained by an unauthorized party when such card information was entered into the payment fields on the website in connection with an online purchase between March 11, 2019 and May 24, 2019. We do not have evidence demonstrating the unauthorized individuals actually obtained this information and we are not aware of any fraudulent transactions at this time. We are nevertheless providing this notice out of an abundance of caution. Purchases through our physical store locations were not impacted by this incident.

What Information Was Involved?

On October 1, 2019, we discovered that the information that may have been acquired in this incident included your name, credit or debit card number, card expiration date and CVV (3 or 4 digit code on the front or back of the card).

What We Are Doing

Because we value our relationship with you, we wanted to make you aware of the incident. We also wanted to let you know what we are doing to further secure your information, and suggest steps you can take. Since learning of the incident, we have implemented enhanced security safeguards to help protect from similar intrusions. We are conducting ongoing monitoring of our website and payment portal to ensure that they are secure and cleared of any malicious activity.

What You Can Do

Below you will find precautionary measures you can take to protect your personal information. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

As a best practice, you should also call your bank or card issuer if you see any suspicious transactions. The policies of the payment card brands such as Visa, MasterCard, American Express and Discover provide that you are not liable for any unauthorized charges if you report them in a timely manner. You should also ask your bank or card issuer whether a new card should be issued to you.

For More Information

Your trust is a top priority for us, and we deeply regret the inconvenience this may have caused. The privacy and protection of our customers' information is a matter we take seriously.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, [REDACTED]

Sincerely,

[REDACTED]

Wolff Shoe Company

- OTHER IMPORTANT INFORMATION -

You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized activity. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported.

In addition, you may contact the Federal Trade Commission (FTC) or law enforcement, such as your state attorney general, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission 600
Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
<https://www.identitytheft.gov/>

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain credit reports from each nationwide credit reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right under the federal Fair Credit Reporting Act (FCRA) to request that the credit reporting agency delete that information from your credit report file.

In addition, under the FCRA, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at <https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf>, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major credit reporting agencies to request a copy of your credit report.

Place a Fraud Alert or Security Freeze on Your Credit Report File

In addition, you may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last 1 year. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

Also, you can contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report, *at no charge*. A security freeze prohibits a credit reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. The credit reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

You may contact the nationwide credit reporting agencies at:

Equifax

P.O. Box 105788
Atlanta, GA 30348
(800) 525-6285
www.equifax.com

Experian

P.O. Box 9554
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
(800) 680-7289
www.transunion.com