



May 7, 2019

Michael J. Waters
312-463-6212
312-819-1910
mwaters@polsinelli.com

**VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)
AND FEDERAL EXPRESS**

The Honorable Gordon MacDonald
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of a Data Security Incident

Dear Attorney General MacDonald:

We represent Simon Pearce (US) Inc. ("Simon Pearce) in connection with an incident that involved the personal information of eleven (11) New Hampshire residents and provide this notice on behalf of Simon Pearce pursuant to N.H. REV. STAT. ANN. § 359-C:20. This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While Simon Pearce is notifying you of this incident, Simon Pearce 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

Simon Pearce recently learned that an unauthorized third party injected malicious code into Simon Pearce's E-commerce platform. The code was removed as soon as it was discovered but could have been able to collect information that customers entered on the website's check-out page while it was active on the platform. That information included customers' names, addresses, and credit or debit card information including CVV code. The incident did not impact any Social Security numbers or driver's license information.

At this point, Simon Pearce is not aware of any fraud or identity theft to any individual as a result of this incident. Nevertheless, because there was a potential for personal information to have been obtained by an unauthorized party, Simon Pearce is notifying persons who entered personal information on the checkout page during the time the code was active on the platform.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

On March 28, 2019, Simon Pearce determined that eleven (11) New Hampshire residents may have been impacted by this incident. Simon Pearce is notifying impacted residents of the

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Nashville New York Phoenix
St. Louis San Francisco Seattle Washington, D.C. Wilmington

Polsinelli PC, Polsinelli LLP in California



The Honorable Gordon MacDonald
May 7, 2019
Page 2

situation by letter today, May 7, 2019. Enclosed is a copy of the notice that is being sent to the impacted residents via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, Simon Pearce promptly removed the malicious code from its website. It also notified law enforcement and two separate forensic security firms to investigate and confirm the security of its website and other online systems. Simon Pearce also took steps to alert the credit card brands so that they can be on the lookout for fraudulent activity. Finally, it instituted additional security controls and procedures to prevent this type of incident from happening in the future.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

A handwritten signature in black ink, appearing to read "Michael J. Waters".

Michael J. Waters

Enclosure

SIMON PEARCE

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

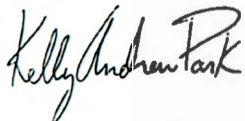
Simon Pearce values and respects the privacy of your information, which is why we are writing to advise you of a recent incident that may have involved some of your personal information. On March 28, 2019 we learned that some of your information could have been obtained by an unauthorized third-party that illegally placed computer code on our e-commerce system.

Upon learning of the incident, we promptly hired a forensic security firm to investigate the incident and have notified law enforcement. We also removed the code from our website and have taken steps to alert the credit card brands of the incident so that they could be on the lookout for fraudulent activity. Finally we have taken additional technical steps to secure our website and prevent this type of incident from occurring in the future.

At this point, we are not aware of any fraud or identity theft to any individual as a result of this incident, and do not know if any personal information was ever actually viewed or acquired by the unauthorized party. Nevertheless, we are notifying you about the incident because we determined that you entered some personal information on the checkout page during the time the code was active on our site. This information included your name, address, and your credit or debit card information including your CVV code. The incident did not impact your Social Security Number or driver's license information.

We value the trust you place in us to protect your privacy, take our responsibility to safeguard personal information seriously, and apologize for any inconvenience or concern this incident might cause. For further information and assistance, please call 1-???-???-???? from 9:00 a.m. to 6:30 p.m. Eastern Time.

Sincerely,



Kelly Park, Director of eCommerce

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by 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 www.annualcreditreport.com/cra/requestformfinal.pdf.

Alternatively, you may 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 as follows:

Equifax

1-800-349-9960
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian

1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion

1-800-888-4213
www.transunion.com
P.O. Box 1000
Chester, PA 19016

Fraud Alerts: 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 (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze

1-800-349-9960
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze

1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze

1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 220 St. Paul Place, Baltimore, MD 21202, (888) 743-0023.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226.

Rhode Island Residents: We believe that this incident affected eight Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400