HISTORICAL EMPORIUM, INC.

June 4, 2019

Gordon MacDonald
Office of the Attorney General
33 Capitol St
Concord, NH 0330 I

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

I am writing to inform you of a possible data security incident. Historical Emporium, Inc. learned on May 21, 2019 that an unknown and unauthorized individual had accessed our website and placed unauthorized code in our shopping cart, which may have exposed payment card information of 25 New Hampshire residents. The affected information includes the residents' name, payment card number, billing address and expiration date. No other personal information was exposed.

Historical Emporium is a retailer selling clothing and accessories through the website https://www.historicalemporium.com. On May 21, 2019, Historical Emporium was alerted by our merchant bank of fraudulent activity among previous customers, indicating a data breach. We began an investigation, discovered and removed the unauthorized code, and took immediate steps to secure the affected part of our systems. After this, an internal investigation was conducted to understand the nature and scope of the incident. The investigation and code correction concluded on the same day we discovered the breach, May 21, 2019. Thereafter we have taken additional steps to enhance security and monitoring of sensitive systems. We now limit access to our shopping cart administrative function to only a short list of IP addresses and are monitoring our entire shopping cart code base for any unauthorized changes.

The investigation found that the code had been in place since March 2, 2019, which resulted in the exposure of 25 New Hampshire residents. Historical Emporium notified affected New Hampshire residents on May 31, 2019, via the attached notice.

Please contact me should you have any questions.

Alicia Allen
Historical Emporium, Inc.

Enclosure: Consumer Notification

188 Stauffer Blvd.
San Jose, CA 95125

(408) 280-5855(p)
(408) 280-7379 (f)

Notice of Data Breach

May 31, 2019

Historical Emporium, Inc has recently discovered a data breach that may have involved some of your personal information.

What happened

On May 21, 2019 we learned that some unauthorized code (malware) was present in the portion of our website that processes payment card transactions. After researching this, we discovered that the code had been in place since March 2, 2019, and as a result, your personal information may have been exposed and/or stolen during your purchase from our website.

When we discovered this breach, we took immediate steps to remove the unauthorized code and secure the affected part of our systems. After this, an investigation began to understand the nature and scope of the incident. The investigation and code correction concluded on the same day we discovered the breach, May 21 2019, and thereafter we have taken additional steps to enhance security and monitoring of sensitive systems.

We believe that this malware may have exposed payment card information for approximately 4,500 customers who made purchases using our website between March 2, 2019 through May 21, 2019. We have reported the details of this breach to the payment card brands, as well as to law enforcement, but this notice to you has not been delayed by their investigations.

What information was involved

The malware was designed to steal customers' payment card information, including cardholder name, payment card number, billing address and expiration date. No other personal information was exposed. As a matter of policy, we only gather and store the information we require to process your payment and to provide service on your order(s).

What are we doing

We have identified the security gap that led to this breach, and have taken numerous steps to close this loophole and harden our website security. We believe that it no longer poses a risk to customers shopping on our website. We continue to take steps to enhance the security of our systems to prevent this type of issue from happening again.

What you can do

We encourage you to remain vigilant by reviewing your account statements and credit reports. Please see the additional information below for steps you may take to protect your information. If you believe there is any unauthorized charges or other activity on your card, please contact your card issuer immediately. Customers are not responsible for counterfeit charges on their credit or debit cards when they are reported in a timely fashion.

For more information

We take our responsibility to safeguard personal information seriously. We regret any inconvenience or concern this incident may cause you, and remain committed to protecting the privacy and security of personal information.

If you have any questions about this situation, please contact us at security@historicalemporium.com or (800) 997-4311, Monday through Friday, 9 a.m. through 4 p.m. PT.

Sincerely,

Alicia Allen
President

Additional Information

How to Request a Credit Fraud Alert and Security Freeze

It is important to monitor your credit and be aware of unusual or fraudulent activity on any of your accounts. Here is some information on how to request a fraud alert and ask for a credit freeze, along with contact information for the three major national credit reporting agencies ("CRAs"), Equifax, Experian and TransUnion. There are differences between how the CRAs handle fraud alerts and security freezes, so please read this carefully.

Fraud Alert

There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any one of the three national CRAs:

Equifax
P.O. Box 740256
Atlanta, GA 30348
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
www.transunion.com

Security Freeze

You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, 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 a freeze. If you place a security 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 security freeze may delay your ability to obtain credit.

There is no fee to place, lift, or remove a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the CRAs at the addresses below:

Equifax
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
www.transunion.com

The CRAs have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. They must also send written confirmation to you within five business days and provide you with a unique PIN or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security Number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your

request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Federal Trade Commission Information

You have rights under the federal Fair Credit Reporting Act. These include, among others, the right to know what is in your credit file; the right to dispute incomplete or inaccurate information; and the right to ask for a credit score.

You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft. The FTC can be reached at the address below:

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

Additional Information for CA, IA, KY, MD, NC, OR, and RI Residents

California: Visit the California Office of Privacy Protection (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

Kentucky: You may obtain information from the Kentucky Attorney General's office, which can be reached at:

Office of the Attorney General of Kentucky
700 Capitol Avenue, Suite 118
Frankfort, KY 40601
502-696-5300

Iowa: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at:

Office of the Attorney General of Iowa
Hoover State Office Building
1305 E Walnut Street
Des Moines, IA 50319
(515) 281-5164
www.iowaattorneygeneral.gov

Maryland: You may obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
888-743-0023
410-576-6300
www.oag.state.md.us

North Carolina: You may contact the North Carolina Attorney General at:

North Carolina Office of the Attorney General
9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
https://www.ncdoj.gov

Oregon: Oregon residents can contact the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
(877) 877-9392
https://www.doj.state.or.us/

Rhode Island: Rhode Island residents can contact the Rhode Island Office of the Attorney General at:

Office of the Attorney General,
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401) 274-4400
http://www.riag.ri.gov.

Rhode Island residents have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to $5 to place a security freeze on your account, and may require that you provide certain personal information (e.g., Social Security number, date of birth, and address) and proper identification (e.g., copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift, or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

Other states: you can find information on how to contact your state attorney general at www.naag.org/naag/attorneys-general/whos-my-ag.php

Click Here to be removed from this list