

June 22, 2020

Attorney General Gordan J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

RECEIVED

JUN 25 2020

CONSUMER PROTECTION

**RE: Mattress Insider, LLC ("MI")
Breach of Personal Information Notification**

Dear Attorney General MacDonald:

In accordance with New Hampshire Revised Statutes Section 359-C:20 Notification of Security Breach Required, we are required to report a security breach of computerized data containing personal information.

What happened?

On or about May 14, 2020 MI was notified by our credit card acquirer, WorldPay, regarding fraudulent charges on cardholders' credit card accounts. As part of the investigation conducted, it was determined that unauthorized access to cardholders' personal information and credit card data may have been compromised from January 11, 2020 through May 14, 2020. Seven (7) New Hampshire residents may have been affected.

An unauthorized entity added malicious script to MI's payment gateway at mattressinsider.com. Malicious script potentially sent consumers' payment card data to an unauthorized third-party website. MI has no association with the third-party website. MI is notifying those who made a payment card transaction on mattressinsider.com while the threat was present.

What Information Was Affected?

MI is unable to know with certainty what customer data was compromised. Customer data that may have potentially been involved is as follows: first and last name, billing address, shipping address, phone number, email address, payment card data (account number, card expiration date and security code).

What We Are Doing.

MI takes the confidentiality, privacy, and security of information in our care seriously. Potential affected individuals are being notified because their personal information including payment card data may have been subject to unauthorized access. The consumer notifications were sent via U.S. Mail on or about June 15, 2020 through June 17, 2020. A template copy of the notification sent to the affected New Hampshire residents is enclosed.

MI has in place security measures to safeguard information and data on our systems and continue to assess and update security measures to safeguard the privacy and security of the information and data in our care.

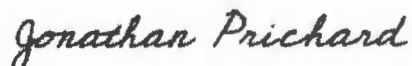
MI identified and removed the extra code that was added to the compromised files which re-routed payment card data and personal information. We searched server logs to identify additional threats. The payment gateway and check out module credentials were changed for all staff. We added additional monitoring to our systems.

We suspect that payment gateway developers may have been involved, we have terminated the business relationship and completed migration to another payment gateway provider as of June 14, 2020.

MI reported the incident to the FBI. At the suggestion of the FBI, MI filed a complaint with Internet Crime Complaint Center (IC3). MI also contacted the Jefferson County Sheriff's department. This notice has not been delayed by a law enforcement investigation.

Although no social security numbers were involved in this incident, MI is offering to all potentially affected individuals access to twelve months of complimentary credit monitoring with fraud alert and identity theft protection services/insurance up to \$25,000 through Equifax. The cost of this service will be paid for by MI.

Sincerely,



Jonathan Prichard
Founder & CEO
Mattress Insider, LLC

Re: Notice of Data Security Event

Dear

Mattress Insider, LLC ("MI") is writing to inform you of a recent event that may impact the privacy of some of your personal information. We want to provide you with information about the event, our response, and steps you may take to better protect against potential misuse of your information.

What Happened?

On or about May 14, 2020 MI was notified by our credit card acquirer, WorldPay, regarding fraudulent charges on cardholders' credit card accounts. As part of the investigation conducted, it was determined that unauthorized access to your personal information and credit card data may have been compromised from January 11, 2020 through May 14, 2020.

An unauthorized entity added malicious script to our payment gateway at mattressesinsider.com. Malicious script potentially sent consumers' credit card information to an unauthorized third-party website. We have no association with the third-party website. MI is notifying those who made a payment card transaction on mattressesinsider.com while the threat was present.

What Information Was Affected?

MI is unable to know with certainty what customer data was compromised. Customer data that may have potentially been involved is as follows: first and last name, billing address, shipping address, phone number, email address, payment card data (account number, card expiration date and security code).

What We Are Doing.

MI takes the confidentiality, privacy and security of information in our care seriously. You are being notified because your personal information may have been subject to unauthorized access.

We have in place security measures to safeguard information and data on our systems. We continue to assess and update security measures to safeguard the privacy and security of the information and data in our care.

MI reported the incident to the FBI. At the suggestion of the FBI, MI filed a complaint with Internet Crime Complaint Center (IC3). MI also contacted the Jefferson County Sheriff's department. This notice has not been delayed by a law enforcement investigation.

We identified and removed the extra code that was added to the compromised files which re-routed credit card information. We searched server logs to identify additional threats. The payment gateway and check out module credentials were changed for all staff. We added additional monitoring to our systems.

What You Can Do.

MI is offering you access to twelve months of complimentary credit monitoring with fraud alert and identity theft protection services/insurance up to \$25,000 through Equifax. The cost of this service will be paid for by MI. Enclosed, for your convenience, is an instruction sheet on how to enroll in the credit monitoring and identity protection services/insurance. You may also access the Enrollment link at www.myservices.equifax.com/efx1_bresngis to enroll online. There is a 4 Step enrollment process which includes Identity Authentication, there will be a series of questions regarding your credit file that you must answer accurately to activate the product.

We strongly encourage you to remain vigilant against incidents or identity theft and fraud by reviewing your account statements and to monitor your credit reports for suspicious activity. We have attached ""TAKING STEPS TO PROTECT YOUR INFORMATION"" which contains suggested guidance how to protect against potential misuse of your information.

For More Information.

We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions or need assistance, please call 844-959-0473 the hours of 9:00 a.m. to 9:00 p.m. EST Monday – Friday and 9:00 am – 6:00 pm EST Saturday and Sunday

Sincerely,

Jonathan Prichard

Jonathan Prichard
Founder & CEO
Mattress Insider, LLC

“TAKING STEPS TO PROTECT YOUR INFORMATION”

Fraud Alert

1. Place an initial Fraud Alert with the Credit Reporting Agencies

The Federal Trade Commission (FTC) recommends that a fraud alert be placed with the Credit Reporting Agencies. A fraud alert lets creditors know to contact you before they open any new accounts or change any of your existing accounts. (The contact information for the credit bureaus can be found below.)

An Initial Alert and an Extended Alert are two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud:

Initial 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 is free and stays on your credit report for at least 90 days. The initial fraud alert may be renewed every 90 days.

Extended Alert: You may have an extended alert placed on your credit report with the appropriate documentary proof if you have previously been a victim of identity theft. An extended fraud alert may remain active for up to 7 years.

You can call any one of the three credit reporting agencies at the numbers below to place a fraud alert. The credit bureau you choose to contact is required to notify the other two, which will place an alert on their versions of your credit report as well.

- Proof of identity will be required.
- They may ask for a copy of your notification letter, proof of residence, and other information.
- Make sure the Credit Reporting Agencies have your latest contact information.

Once the alert has been put in place, any business that has been contacted to open a new account for you will be required to contact you and receive proof of your identity first.

2. Place a Freeze on your credit with the Credit Reporting Agencies

You may also place a Freeze on your credit file, known as a Security Freeze. A Freeze prevents new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the Freeze.

A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. (The contact information for the credit bureaus can be found below.)

Be Vigilant

Be vigilant in monitoring your credit and personal information to ensure the criminals have not attempted to use stolen information.

1. Review your bank, credit card and debit card account statements carefully.
2. Monitor your credit reports with the major credit reporting agencies.
 - Once you place the fraud alert in your file, you are generally entitled to order free copies of your credit reports, and, if you ask, only the last four digits of your Social Security Number will appear on your credit reports. Carefully review any credit reports you receive and look for:
 - Accounts you did not open.
 - Inquiries from creditors that you did not initiate
 - Personal information, such as home address and Social Security Number that are not accurate.
 - Re-establish the Fraud Alert every 90 days: Even if you do not find any signs of fraud on your reports, some consumer protection specialists recommend checking your credit report every three months and keeping the Fraud Alert in place.
3. Update or revise User Names and Passwords.

Another area which is often overlooked are usernames and passwords. Update your information for all of your accounts and continue to update these on a regular basis. Stale and/or repetitive passwords are easier to hack.

- Passwords should be a minimum of 8 characters long and be a combination of upper case letters, lower case letters, numbers, and symbols.
- Don't use family or pet names, birthdates, or other personal information the criminal may have access to.
- Don't use the same passwords on separate accounts.

Immediately Report Any Suspicious Activity

If you detect any suspicious activity on any account, you should promptly notify:

1. The financial institution or company with which the account is maintained;
2. Proper law enforcement authorities: Call your local police or sheriff's office and file a police report of identity theft;
 - If appropriate, give your contact information to the law enforcement agency investigating the incident for the company or organization from whom you received the initial notification;
 - Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.
3. Federal Trade Commission: Create an Identity Theft Report. (Instructions are found below) Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.
4. Credit report agencies: Call the credit agency at the telephone number on your credit reports or as listed below. They may request a copy of your police report, and if you have it, the Identity Theft Report.
5. Your State Attorney General: Almost every state is actively working to help stop identity theft and has laws in place regarding company, organization, and agency involvement in notifying you of possible breaches. You may notify them if you are a victim of identity theft.

Credit card companies, banks, and other financial institutions may notice attempts to access your information or accounts before you do. If you receive a notice from them, promptly follow their instructions.

Credit Reporting Agencies (a.k.a. Consumer Credit Bureaus)

You may obtain a free copy of your credit report from each of the three major credit reporting agencies by visiting <http://www.annualcreditreport.com>, calling toll-free 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/cra/requestformfinal.pdf>.

Direct contact information for the three national credit reporting agencies:



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



Experian
(888) 397-3742
www.experian.com
P.O. Box 9532
Allen, TX 75013



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

Federal Trade Commission

To report fraud, identity theft, or an unfair business practice, visit the FTC website ftc.gov/complaint and select "identify theft" as the complaint type. You will be asked a series of questions. If possible, be prepared to provide:



at
asked a

- Your contact information: name, address, phone number, email
- Information about the breached company or seller: business name, address, phone number, website, email address, representative's name
- Details about the possible use of your identity and what accounts may be affected.

Additional information regarding steps to preventing identify theft can be found at ftc.gov/idtheft or you can call 1-877-ID-THEFT (877-438-4338).



Enter your Activation Code: <INSERT ACTIVATION CODE>
Enrollment Deadline: <INSERT DATE>

Product Information

Equifax® Credit Watch™ Gold with WebDetect Features

- Equifax® credit file monitoring and alerts to key changes to your Equifax credit report
- Wireless alerts (available online only) Data charges may apply.
- Access to your Equifax credit report
- Internet Scanning¹ Monitors suspicious web sites for your Social Security, Passport, Credit Card, Bank, and Insurance Policy Numbers, and alerts you if your private information is found there.
- Automatic Fraud Alerts² with a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit
- Up to \$25,000 Identity Theft Insurance³
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

Enrollment Instructions

To sign up online for online delivery go to http://myservices.equifax.com/efx1_bresngis

- 1. Welcome Page:** Enter the Activation Code provided at the top of this page in the “Activation Code” box and click the “Submit” button.
- 2. Register:** Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the “Continue” button.
- 3. Create Account:** Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the “Continue” button.
- 4. Verify ID:** The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the “Submit Order” button.
- 5. Order Confirmation:** This page shows you your completed enrollment. Please click the “View My Product” button to access the product features.

¹Internet scanning, will scan for your Social Security number (if you choose to), up to 5 bank account numbers, up to 6 credit/debit card numbers you provide, up to 3 email addresses, up to 10 medical ID numbers, and up to 5 passport numbers. Internet scanning scans thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and is constantly adding new sites to those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that Internet scanning is able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

²The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

³ Identity theft insurance is underwritten by American Bankers Insurance Company of Florida or its affiliates. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.