



Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>

<Name>

<Address1>

<Address2>

<<City>><<State>><<Zip>>

<<Date>>

Dear <Name>,

Notice of Data Breach

Tempur-Pedic recently became aware of a potential security incident possibly affecting the personal information of certain individuals who made a payment card purchase on the Tempurpedic.com website. We are providing this notice as a precaution to inform potentially affected individuals about the incident and to call your attention to some steps you can take to help protect yourself. We sincerely regret any concern this may cause you.

What Happened

We were recently informed by the company that previously hosted our website of a potential security incident involving our website. Based upon the vendor's forensic investigation, it appears that an unauthorized individual was able to gain access to portions of the website and install malicious software on the website servers that was designed to capture historical payment card information provided on the website.

What Information Was Involved

We believe that the incident could have affected certain information (including name, address, email address, telephone number, payment card account number, and expiration date) of individuals who made a purchase on the website. According to our records, you made a payment card transaction on the website and your information may be affected. Please note that because we do not collect sensitive personal information like Social Security numbers for standard payment card transactions, this type of sensitive information was not affected by this incident.

What We Are Doing

We take the privacy of personal information seriously, and deeply regret that this incident occurred. We took steps to address and contain this incident promptly after it was discovered, including initiating an internal investigation into the incident and communicating with the vendor that hosted and operated the website to learn more about what occurred. The vendor informed us that it engaged an outside forensic investigation firm to assist them in investigating and remediating the situation, has removed the malware, and is in the process of deploying file monitoring software and an endpoint security program to enhance the security of all the websites that they host and operate. Note that the Tempur-Pedic website was transitioned to a new hosting vendor in October of 2016, so this incident does not affect any customers who have made purchases on the website after September 30, 2016. In addition, the incident has been reported to federal law enforcement and the vendor is cooperating with their investigation.

In addition, to help protect your identity, we are offering one year of complimentary identity protection services from a leading identity monitoring services company. These services help detect possible misuse of your personal information by monitoring your personal information online and provide you with identity protection support focused on immediate identification and resolution of identity theft. For more information about these services and instructions on completing the enrollment process, please refer to the information in the "Information about Identity Theft Protection" reference guide included here.

What You Can Do

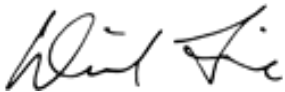
We recommend that you review credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. We urge you to remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not recognize, you should immediately notify the issuer of the credit or debit card as well as the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). In instances of payment card fraud, it is important to note that cardholders are typically not responsible for any fraudulent activity that is reported in a timely fashion.

Although Social security numbers were not at risk in this incident, we recommend, as a general practice, that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. As an additional precaution, we are providing information and resources to help individuals protect their identities. This includes an "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection.

For More Information

For more information about this incident, or if you have additional questions or concerns about this incident, you may contact us at 844-319-9624 between 9:00 a.m. and 9:00 p.m. Eastern time, Monday through Friday. Again, we sincerely regret any concern this event may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Dan Fine". The signature is fluid and cursive, with a large initial "D" and "F".

Dan Fine

Vice President, Direct Channels

Information about Identity Theft Protection

To help protect your identity, we are offering a complimentary membership in Experian's® CSID Protector services. These services automatically include Identity Restoration services with no further action required. If you are a victim of fraud, simply call CSID at **(855) 568-2999** by **June 30, 2017** and a dedicated Identity Theft Restoration agent will help you restore your identity.

You can also activate the CyberAgent® Internet Surveillance and Identity Theft Insurance services by enrolling in the CSID Protector services at no cost to you. To enroll:

- Visit <https://en.csidprotector.com/enrollment/1?RTN=90000065> to complete a secure sign up process and answer some questions to confirm your identity.
- Submit your PIN Code: **<Enrollment Code>** This PIN Code can only be used once and cannot be transferred to another individual.
- Activate your CSID Protector coverage by no later than **June 30, 2017**.

Once enrolled, these services are effective for 12 months. For additional information on these services please visit CSID.com.

Review Accounts and Credit Reports: You should regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should also remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

Fraud Alerts: There are also 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: 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 at least 90 days. 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 of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Credit Freezes: You may have the right to put 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 a 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. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. 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.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)

General Contact:

P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:

P.O. Box 740256, Atlanta, GA 30374

Credit Freezes:

P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)

General Contact:

P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:

P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)

General Contact:

P.O. Box 105281
Atlanta, GA 30348
877-322-8228

Fraud Alerts and Security Freezes:

P.O. Box 2000, Chester, PA 19022

888-909-8872