16365

honeybee

Honeybee Health, Inc.

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Honeybee Health understands the importance of protecting our customers' information. Regrettably, we are writing to inform you of an incident that may have included your name, billing and shipping address, and payment card number, expiration date, and security code (CVV) for the card you used to make a purchase on www.honeybeehealth.com between November 16, 2019 and December 2, 2019. If during that purchase you provided the name of other medications you are taking, medical conditions you have, or the name and contact information for your provider, that information may have also been involved in the incident.

Although this incident only involved a limited number of Honeybee customers, we want to remind you to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. Immediately report any unauthorized charges to your financial institution because the payment card network rules generally restrict cardholder responsibility for fraudulent charges that are timely reported. For additional information about steps you can take, please review the information included with this letter.

We deeply regret any inconvenience or concern this incident may cause you and take this matter very seriously. To help prevent a similar incident from occurring in the future, we are taking steps to enhance our security environment, including moving the server behind additional protective security layers and scanning our website for malicious code.

If you have any questions, please call 1-???-???-????, Monday through Friday, between 9:00 a.m. and 6:30 p.m. Eastern Time.

Sincerely,

Peter Wang
Co-Founder & CEO
Honeybee Health
3515 Helms Avenue
Culver City, CA 90232

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Residents of **Massachusetts** may contact and obtain information from their state attorney general at:

- *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.htm

If you are a resident of Massachusetts, note that pursuant to Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

Fraud Alerts: 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 (1) 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 of the three national credit reporting agencies.

Credit Freezes: 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 that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. 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 or lift 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 credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)

7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

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 place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("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 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 hour 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 hour 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.

Appendix

Honeybee Health is an online pharmacy that verifies, fills, and mails prescription medications to individuals across the United States.

On November 19, 2019, Honeybee Health ("Honeybee"), learned that a small number of its customers experienced unauthorized charges on their payment card after they used the card to make a purchase at honeybeehealth.com (the "Website"). Honeybee immediately launched an internal investigation, and a leading computer forensic firm was hired to assist. The investigation identified that unauthorized code was added to the Website's checkout page on November 16. The code was removed from the Website as soon as it was found on November 19. On November 28, Honeybee was reviewing the Website code and discovered that the unauthorized code had re-appeared. The script was again removed the same day. Shortly thereafter, on December 2, Honeybee found a similar script on the Website. The code was removed and Honeybee moved the affected server behind additional protective security layers.

The unauthorized code was designed to copy information entered during checkout and send the information to an unauthorized person. That information included the name, billing and shipping address, and payment card number, expiration date, and security code (CVV) of certain Honeybee customers that made a purchase between November 16-19, November 23-29, and on December 2, 2019. If the customer also provided the name of other medications he or she is taking, medical conditions that he or she may have, or the name and contact information of his or her provider, that information may have also been obtained by the unauthorized person. The code did not copy order information that was not typed into a text field during the checkout process.

On January 17, 2020, pursuant to M.G.L. c. 93H, § 3(b), Honeybee will begin mailing notification letters via U.S. First-Class mail to 22 Massachusetts residents in substantially the same form as the enclosed letter. In addition, Honeybee has established a dedicated call center where individuals may obtain more information regarding the incident.

To help prevent a similar incident from occurring in the future, Honeybee is taking steps to enhance its security environment, including moving the server behind additional protective security layers and scanning its Website for malicious code.