


Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

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

<<Country>>

<<Date>>

Notice of Data Breach

Dear <<Name 1>>:

Hamilton Beach Brands, Inc. (“Hamilton Beach”) is writing to inform you that we recently identified and addressed a security incident that may have involved your payment card information. This notice explains the incident, the measures we have taken, and additional steps you can take in response.

What Happened?

On February 4, 2021, Hamilton Beach discovered unauthorized computer code on its ecommerce website (www.hamiltonbeach.com). We immediately removed the unauthorized code, began an investigation, and a cybersecurity firm was engaged to assist with our investigation. The code was capable of obtaining information entered by customers during the checkout process and sending that information out of our system. On March 12, 2021, the investigation determined that an unauthorized person could have accessed information entered by some customers during the checkout process for orders attempted or placed between December 18, 2020 and February 4, 2021.

What Information Was Involved?

The information that could have been copied was:

- Contact Information – first and last name, shipping and billing address, email address, and phone number;
- Payment card information – payment card number, expiration date, and card verification code for the payment card ending in <<Variable Data>>.

What We Are Doing.

In addition to conducting an investigation, Hamilton Beach has notified law enforcement and is cooperating with their investigation. We notified the payment card networks so that they can inform the banks that issued the cards. We also worked to ensure the unauthorized person was no longer able to collect customer information and are taking measures to enhance the security of our site.

What You Can Do.

We encourage you to closely review your payment card statements for any unauthorized charges. You should immediately report unauthorized charges to the bank that issued your card because payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported. Please see the additional information attached to this letter for additional steps you may take.

More Information.

We regret that this occurred and apologize for any inconvenience. If you have any further questions or concerns, we established a dedicated call center, which can be reached by calling 855-654-0889 Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

A handwritten signature in black ink that reads "Chuck Vion, B." The signature is written in a cursive style.

Chuck Vion
Senior Manager, Digital Marketing

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

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general 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.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? 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

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.