

BakerHostetler

Baker&Hostetler LLP

811 Main Street
Suite 1100
Houston, TX 77002-6111

T 713.751.1600
F 713.751.1717
www.bakerlaw.com

Jennifer E. Costa
direct dial: 713.646.1344
jcosta@bakerlaw.com

April 9, 2021

VIA E-MAIL (DOJ-CPB@DOJ.NH.GOV)

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, Hamilton Beach Brands, Inc. (“HBB”) to notify you of a security incident involving 39 New Hampshire residents.

On February 4, 2021, HBB discovered unauthorized computer code on one of its ecommerce websites (www.hamiltonbeach.com). Upon discovery, it immediately removed the unauthorized code, began an investigation and contacted law enforcement and payment card networks. BakerHostetler was engaged to advise on potential notification obligations and it engaged a cybersecurity firm to assist with the investigation. On March 12, 2021, the investigation determined that an unauthorized person could have obtained the payment information entered by some customers during the checkout process for orders attempted or placed on hamiltonbeach.com between December 18, 2020 and February 4, 2021. The information that could have been copied was name, shipping and billing address, email address, phone number, payment card number, expiration date and CVV.

HBB began mailing notification letters via U.S. mail on April 9, 2021, to the 39 New Hampshire residents involved, in accordance with N.H. Rev. Stat. Ann. § 359-C:20,¹ in substantially the same form as the enclosed letter. HBB is encouraging the individuals to closely review their payment card statements and report any unauthorized charges to the bank that issued

¹ This notice does not waive HBB’s objection that New Hampshire lacks personal jurisdiction over it regarding any claims relating to this incident.

April 9, 2021

Page 2

the card. It has also established a dedicated phone number where individuals can obtain additional information regarding the incident.

To help prevent this type of incident from happening again, HBB implemented additional security measure and continues to look for opportunities to enhance its security measures.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in black ink, consisting of several overlapping loops and a long horizontal stroke extending to the right.

Jennifer E. Costa
Counsel

Enclosure


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>>

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.

For 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 cursive script that reads "Chuck Vion, Jr.".

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.

Additional information for residents of the following states:

*Hamilton Beach is located at 4421 Waterfront Drive Glen Allen, VA 23060.
1 (800) 851-8900*

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves **XX** individuals in Rhode Island. Under Rhode Island 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, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

New Mexico: A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.