

# Hamilton Beach

Dana B. Sykes · Assistant General Counsel

January 12, 2011

OFFICE OF THE ATTORNEY GENERAL  
CONSUMER PROTECTION AND ANTITRUST BUREAU  
33 CAPITOL STREET  
CONCORD, NEW HAMPSHIRE 03301

Dear Sir or Madam:

Pursuant to applicable state law, this letter is to inform you that Hamilton Beach Brands, Inc. ("Hamilton Beach") recently experienced a data security breach on its e-commerce site server. Hamilton Beach has reason to believe that the personal information of one of its online customers who reside in the State of New Hampshire may have been accessed on the afternoon of January 5, 2011 without proper authorization. The personal information affected may include customer name, address, telephone number, email, and credit card information. To date, Hamilton Beach is not aware of any fraudulent credit card transactions as a result of this incident.

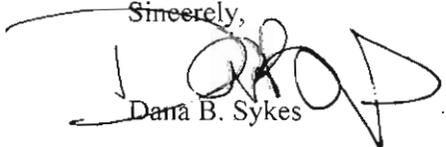
On January 5, 2011, we discovered that hacker code had been placed on a dedicated server capturing the Personal Information of 24 consumers who had tried to place orders on the [www.hamiltonbeach.com](http://www.hamiltonbeach.com) or [www.proctorsilex.com](http://www.proctorsilex.com) websites. Our investigation revealed that the Personal Information was captured during the order entry process prior to encryption and transmittal for processing. Our investigation further revealed that the captured Credit Card Data was sent to the following two email accounts:  
[hmtbccv@gmail.com](mailto:hmtbccv@gmail.com)  
[prosilexsccv@gmail.com](mailto:prosilexsccv@gmail.com)

Once discovered, Hamilton Beach immediately undertook the following actions: shut down the subject websites; contacted consumers affected by email and telephone; immediately began an investigation which is ongoing at this time; implemented an immediate code scan check to identify the hacker code used to capture this information; eliminated the hacker code from the subject server; notified the FBI; notified Google and notified each affected customer's credit card company.

Hamilton Beach's investigation of this incident is ongoing. In addition to continuing its investigation, Hamilton Beach has sent a supplemental notice to the one all affected New Hampshire resident, a copy of which is enclosed.

Hamilton Beach believes this letter is compliant with the notice requirements under applicable state law. If, however, you require additional information or documentation, please do not hesitate to contact me by telephone at (804) 527-7137 or by e-mail at [dana.sykes@hamiltonbeach.com](mailto:dana.sykes@hamiltonbeach.com).

Sincerely,

  
Dana B. Sykes

# Hamilton Beach

January 12, 2011.

Dear [REDACTED]:

This letter is being sent in follow-up to the email and voice mail you received from Hamilton Beach Brands, Inc. (Hamilton Beach) on January 5, 2011 informing you that your personal information - name, address, telephone number, email address and [REDACTED] credit card information may have been accessed, on or about January 5, 2011 without proper authorization.

Upon learning of this potential unauthorized access, Hamilton Beach took the following actions: shut down the subject website; contacted consumers affected by email and telephone; immediately began an investigation which is ongoing at this time; implemented an immediate code scan check to identify the hacker code used to capture this information; eliminated the hacker code from the subject server; notified the FBI; and notified the your credit card company.

The subject credit card was not charged for orders on **proctorsilex.com** and to date Hamilton Beach is unaware of any incidents of fraudulent use of such credit card information, or of any cases of identity theft related to this incident.

We strongly encourage you to remain alert in guarding your personal information by regularly reviewing your account statements and monitoring your credit reports. In addition, you may consider undertaking one or more of the following actions:

- ❖ **Obtain or File a Police Report** – If Hamilton Beach files a police report in your jurisdiction, you have a right to obtain it. You also have the right to file a police report.
- ❖ **Place a Fraud Alert on Your Credit File** - A fraud alert tells creditors to take extra precautions before they open any new accounts or change any existing accounts. A fraud alert can be placed by calling the Automated Fraud Alert systems at the numbers below for any one of the three credit reporting agencies. You only need to contact one of the three credit reporting agencies; your request will be shared electronically with the other two agencies.
- ❖ **Place a Security/Credit Freeze on Your Credit File** - A security/credit freeze prevents third parties from accessing your credit report without your consent. A security freeze must be placed with each of the three credit reporting agencies for it to appear in their records. Because a security freeze can hinder one's ability to obtain credit, all three agencies recommend that applicants plan ahead before placing the freeze.

Under New Hampshire law, if you are a victim of identity theft and you submit or have previously submitted a copy of a valid police report, investigative report or complaint filed with a law enforcement agency about the unlawful use of your personal information by another person, no fees will be charged to place a security freeze on your credit file. The mechanism for requesting a security freeze and the information required differs for each credit reporting agency:

- **Equifax** – You must submit a written request that includes your name, address, date of birth and Social Security Number, proof of current address (such as a current utility bill), and, if required, payment of applicable fees. Personal checks, American Express, Mastercard, VISA, and Discover Cards are acceptable forms of payment. If you are required to pay and are paying by credit card, you must include the following information:

- Name of the person as it appears on the credit card
- Type of credit card (American Express, Mastercard, VISA, or Discover Card)
- Card number
- Expiration date (month and year).
- Card Identification Number (for American Express: – the 4 digit number on the front of card above the account number; for Mastercard, VISA, or Discover Card: the 3 digit number on back of card at the end of the account number).

If you are an identity theft victim and are requesting a security freeze, you must also include a copy of a police report, identity theft report, or other government law enforcement agency report, such as a DMV report.

All written requests must be sent to: **Equifax Security Freeze, P.O. Box 105788, Atlanta, Georgia 30348.**

- **TransUnion** – You may submit a request in one of three ways:

- Online: <https://annualcreditreport.transunion.com/fa/securityFreeze/indexProcess>
- By Telephone: 1-888-909-8872.
- By Mail:
  - Requests sent by regular mail should be mailed to the following address:  
**TransUnion, Fraud Victim Assistance Department, P.O. Box 6790 Fullerton, CA 92834.**
  - Requests sent by overnight mail should be mailed to the following address:  
**TransUnion, Fraud Victim Assistance Department, 1561 E. Orangethorpe Ave. Fullerton, CA 92831.**

Your request must include your name, address, Social Security Number, and a credit card number (American Express, Discover, MasterCard and Visa) with expiration date to pay

the applicable fee, if any, for the service. You must also include proof of your current residence, such as a state issued identification card or driver's license.

If you are an identity theft victim and are requesting a security freeze, you must also include a copy of a police report, identity theft report, or other government law enforcement agency report, such as a DMV report.

➤ **Experian** – You may submit a request in one of two ways:

- **Online:** [www.experian.com/freeze](http://www.experian.com/freeze)
- **By Mail:**
  - Requests should be sent by certified mail to the following address: **Experian, P.O. Box 9554, Allen, TX, 75013.**

Your request must include your full name, with middle initial and generation (e.g. Jr., Sr., II, III, etc.); Social Security number; date of birth (month, day and year); current address and previous addresses for the past two years; one copy of a government issued identification card (e.g. driver's license, state or military ID card, etc.); one copy of a utility bill, bank or insurance statement, etc.; and a check or money for \$5.00 or a valid investigative or incident report or complaint with a law enforcement agency or the DMV.

❖ **Report Suspicious Activity on Your Credit Card and Other Account Statements** - If you find suspicious activity on your account statements or credit report or have reason to believe your information is being misused, we urge you to call your local law enforcement agency to file a police report. You should obtain a copy of the police report since many creditors want the information it contains to address fraudulent debts. Also, as previously mentioned, many credit reporting agencies require it to place a free security freeze on your credit file. You may notify the three major credit reporting agencies about the police report using the contact information below:

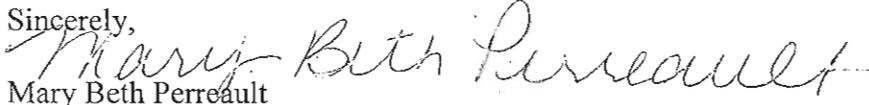
<p><b>Equifax Fraud Division</b>            P.O. Box 740250            Atlanta, GA 30374  <a href="http://www.equifax.com">www.equifax.com</a></p>	<p><b>TransUnion Credit Bureau</b>            P.O. Box 6970            Fullerton, CA 82834  <a href="http://www.transunion.com">www.transunion.com</a></p>	<p><b>Experian</b>            P.O. Box 9532            Allen, TX 75013  <a href="http://www.experian.com">www.experian.com</a></p>
<p><b>Automated Fraud Alert</b></p> <ul style="list-style-type: none"> <li>• <a href="http://www.fraudalerts.equifax.com">www.fraudalerts.equifax.com</a></li> <li>• 1.800.525.6285</li> </ul> <p><b>Order Free Credit Report</b></p> <ul style="list-style-type: none"> <li>• 1.877.322.8228</li> <li>• <a href="http://www.annualcreditreport.com">www.annualcreditreport.com</a></li> <li>• Annual Credit Report Request Service            P.O. Box 105281            Atlanta, GA 30348-5281</li> </ul>	<p><b>Automated Fraud Alert</b></p> <ul style="list-style-type: none"> <li>• 1.800.680.7289</li> <li>• Email:  <a href="mailto:fvad@transunion.com">fvad@transunion.com</a></li> <li>• Mail</li> </ul> <p><b>Order Free Credit Report</b></p> <ul style="list-style-type: none"> <li>• <a href="http://www.annualcreditreport.com">www.annualcreditreport.com</a></li> <li>• 1.800.888.4212</li> <li>• 1-877-322-8228</li> <li>• Annual Credit Report Request Service</li> </ul>	<p><b>Automated Fraud Alert</b></p> <ul style="list-style-type: none"> <li>• <a href="https://www.experian.com/fraud/center.html">https://www.experian.com/fraud/center.html</a></li> <li>• 1.888.397.3742</li> </ul> <p><b>Order Credit Report</b></p> <ul style="list-style-type: none"> <li>• 1.888.397.3742</li> <li>• <a href="http://www.annualcreditreport.com">www.annualcreditreport.com</a></li> <li>• Annual Credit Report Request Service            P.O. Box 105281            Atlanta, GA 30348-5281</li> </ul>

	P.O. Box 105281 Atlanta, GA 30348-5281	
--	---	--

Finally, if you suspect you are a victim of identify theft, we encourage you to file a complaint with the Federal Trade Commission (FTC) at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) or at 1-877-ID-THEFT (438-4338). The FTC offers consumer assistance and educational materials relating to identity theft and privacy issues. The complaint will be accessible to law enforcement for their investigations.

We sincerely apologize to you for this situation and want to assure you that protecting the security and privacy of your information remains our top priority. We have made and will continue to make significant investments in security software, systems and procedures, and will remain vigilant in protecting you. For more information, contact me by telephone at 1-804-418-8868 or by e-mail at [marybeth.perreault@hamiltonbeach.com](mailto:marybeth.perreault@hamiltonbeach.com). You may also contact Dana Sykes, Assistant General Counsel by telephone at 1-804-527-7137 or by email at [dana.sykes@hamiltonbeach.com](mailto:dana.sykes@hamiltonbeach.com). Once again, please be assured that your security and privacy are our top concern.

Sincerely,

  
Mary Beth Perreault

Senior Manager, Corporate Communications