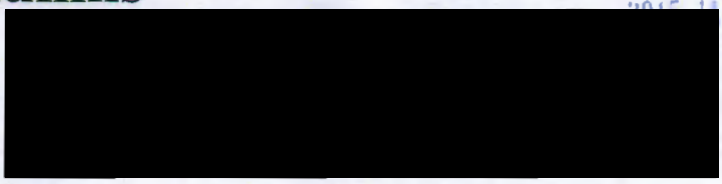
Nelson Mullins



January 16, 2015

Via Electronic Mail & Certified U.S. Postal Mail

The Honorable Joseph Foster
Office of the Attorney General of New Hampshire
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301
Email: attorneygeneral@doj.nh.gov

Re: Data Breach Notification

Dear Attorney General Foster:

We are writing to notify you concerning the personal financial information of 416 New Hampshire residents who are customers of our client, Barbecue Renew, Inc. ("Barbecue Renew"). Barbecue Renew has confirmed a data security incident that may affect these residents. Between January of 2014 to October 2014, the customers' personal financial information may have been accessed by parties outside of our client's organization. The types of vulnerable data included: first and last name, address, personal card account number, expiration data, and card security codes. In October of 2014, Barbecue Renew received a notification from its acquiring bank of at least two incidents of possible fraud associated with a suspected security compromise of cardholder data stored by Barbecue Renew. By October 21, 2014, Barbecue Renew had remedied the vulnerability that was suspected of having been exploited by the attackers by either removing or fixing vulnerable web pages but attackers had already exploited this vulnerability. On November 12, 2014, Barbecue Renew was informed of a third potential compromise of cardholder data by a third payment card brand.

Barbecue Renew immediately notified law enforcement and took immediate steps to investigate the information that may have been accessed and the extent of any possible compromise of cardholder data. It immediately engaged a third party forensic investigator to conduct a comprehensive review of its security environment and to investigate the source of the suspected vulnerability and compromise.

Through the investigation, Barbecue Renew discovered that from January of 2014 to October 2014, cardholder data was exposed on three separate occasions for various lengths of time due to an SQL injection cyber attack against its web server. On December 17th, 2014, Barbecue Renew provided a final investigative report to the card brands and Bank of America, its acquiring bank, to alert them of the results of the investigation and to confirm that individual personal financial information was compromised. Barbecue Renew is working with leading IT security firms, data privacy and protection attorneys, law enforcement and payment industry contacts to conduct a thorough investigation of the incident. Additionally, Barbecue Renew is devoting all necessary resources to its ongoing efforts to enhance its information security policies and procedures in light of this incident to minimize the risk of such incidents in the future.

Barbecue Renew will provide written notification using a specialized firm, Kroll, within 7 days of the date of this letter, by U.S. first class mail to all affected residents to the last address our client has on record, and a sample of this notification letter is enclosed. Barbecue Renew will also be providing the attached "Frequently Asked Questions" as a guide to help these customers best determine what to do as a result of this notification. Finally, attached please find a copy of the notification Barbecue Renew will be providing to consumer reporting agencies of the security breach.

The services from Kroll will also include a toll-free number for recipients to call with questions. Additionally, Barbecue Renew, through Kroll, will be providing the affected individuals with 1-year of free credit monitoring services.

Barbecue Renew will continue to improve its privacy, security, and related risk management programs and will continue to work with its employees to ensure that incidents such as this will not happen again.

DFK:df
Enclosures: Sample Consumer Notification Letter
Frequently Asked Questions

cc: Mr. Dennis Soltis,
Mr. Martin Soltis

grillparts.com

<<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

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

Dear <<MemberFirstName>> <<MemberLastName>>,

Barbecue Renew, Inc., ("Barbecue Renew" or "us" or "we"), is an e-commerce retailer offering grill accessories, equipment and replacement parts through our website www.grillparts.com. You are receiving this notification because at some point in the past, you completed a purchase through our website which required you to provide us with your credit card information. We have determined that your cardholder data, which may include your first and last name, address, personal card account number, expiration date, and card security codes, may have been compromised as a result of a series of cyber attacks on our web server. This letter will explain how this compromise occurred, how you could potentially be affected, and what specific steps you may take in order to protect yourself from certain risks regarding any potential misuse of this information.

In October of 2014, we received a notification from our acquiring bank, Bank of America, of two incidents of possible fraud associated with a suspected security compromise of cardholder data. We immediately began an internal investigation and took corrective measures to remediate any possible vulnerability which may have been exploited by attackers thereby resulting in a security breach. By October 21, 2014, Barbecue Renew had remedied the vulnerability that was suspected of having been exploited by the attackers by either removing or fixing vulnerable web pages but attackers had already exploited this vulnerability.

On November 12, 2014, Barbecue Renew was informed of a third potential compromise of cardholder data by a third payment card brand. Unfortunately, this occurred prior to our implementation of the previously described corrective measures. Barbecue Renew immediately notified law enforcement, retained a third party forensic investigator and took immediate steps to determine what information may have been accessed and the extent of any possible compromise of cardholder data.

Through the investigation we discovered that from January of 2014 to October 2014, cardholder data was exposed on three separate occasions for various lengths of time due to a cyber attack against our web server. On December 17th, 2014, Barbecue Renew provided a final investigative report to the card brands and Bank of America, its acquiring bank, to alert them of the results of the investigation and to confirm that individual personal financial information was in fact compromised. We are working with leading IT security firms, data privacy and protection attorneys, law enforcement and payment industry contacts to continue to address this incident. Additionally, we are devoting all necessary resources to our ongoing efforts to enhance our information security policies and procedures in light of this incident to minimize the risk of such incidents in the future.

We are notifying you so that you can take steps to help protect your information from unauthorized use, such as the steps detailed in the enclosed reference guide. We also want to assure our customers we are working hard to address these events and will share additional facts as we are able to do so. If you have specific questions related to the security of your card holder information in light of this notification you should contact your card issuing bank directly.

We urge you to be vigilant about monitoring unauthorized account activity and to alert your bank and/or account issuers who may be able to impose additional security measures. We are also working with Kroll to provide you with services at no cost to you to help you safeguard your identity, including consultation and restoration services in the event of a potential identity theft.

What Are We Doing To Protect You?

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide **identity theft protection at no cost to you for one year.** Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

Your identity theft protection services include Credit Monitoring, Web Watcher, Identity Theft Consultation and Restoration. Additional information describing your services is included with this letter.

Visit kroll.idMonitoringService.com and follow the online instructions to take advantage of your Identity Theft Protection Services.

Membership Number: <<Member ID>>

What Should You Do If You Have Any Questions Or Feel You Have An Identity Theft Issue?

Call 1-???-???-????, 8 a.m. to 5 p.m. (Central Time), Monday through Friday. Kroll's licensed investigators are standing by to answer your questions or help you with concerns you may have. *Please have your membership number ready.*

We sincerely apologize for any inconvenience this incident may cause you.

Sincerely,

Barbecue Renew

kroll.idMonitoringService.com is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox and Safari.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. To receive credit services by mail instead of online, please call 1-???-???-????.

Reference Guide

To protect against possible identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, to monitor your credit reports and to consider these additional steps:

Security Freeze. Some state laws allow you to place a security freeze on your credit reports. This would prohibit a credit reporting agency from releasing any information from your credit report without your written permission. You should be aware, however, that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services. The specific costs and procedures for placing a security freeze vary by state law, but this reference guide provides general information. You can find additional information at the websites of any of the three credit reporting agencies listed below.

If you believe that you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, it will not charge you to place, lift or remove a security freeze on your credit reports. In all other cases, a credit reporting agency may charge you up to $5.00 (and in some cases, up to $20.00) each time you place, temporarily lift, or permanently remove a security freeze.

Requirements vary by state, but generally to place a security freeze on your credit report, you must send a written request to each of the three credit reporting agencies noted below, which must include the following information: (1) Full name (including middle initial as well as Jr., Sr., II, III, etc.); (2) Social Security Number; (3) Date of birth; (4) Addresses for the prior five years; (5) Proof of current address; (6) A legible copy of a government issued identification card; (7) A copy of any relevant police report, investigative report, or complaint to a law enforcement agency concerning identity theft and (8) If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash though the mail.

Equifax Security Freeze P.O. Box 105788 Atlanta, Georgia 30348 877-478-7625 www.equifax.com	Experian Security Freeze P.O. Box 9554 Allen, Texas 75013 888-397-3742 www.experian.com	TransUnion Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790 800-680-7289 www.transunion.com

Free Credit Reports. To order a free copy of your credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three national credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

Fraud Alerts. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert alerts you of an attempt by an unauthorized person to open a new credit account in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a free fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three credit bureaus. You can also place a fraud alert on your credit report online at the websites listed below for Equifax and Experian and via email for TransUnion at fvad@transunion.com.

Equifax P.O. Box 105069 Atlanta, Georgia 30348-5069 800-525-6285 www.fraudalerts.equifax.com	Experian P.O. Box 1017 Allen, Texas 75013 888-397-3742 www.experian.com	TransUnion Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790 800-680-7289 www.transunion.com

Police Report. If you find suspicious activity on your credit reports or account statements, or have reason to believe that your personal information is being misused, contact your local law enforcement authorities immediately and file a police report. You have the right to request a copy of the police report and should retain it for further use, as many creditors want the information it contains to absolve you of potential fraudulent debts.

Consulting the FTC. In addition to your state Attorney General, you can contact the FTC to learn more about how to protect yourself from identity theft:

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

Kroll.

Take Advantage of Your Identity Theft Protection Services

You've been provided with access to services from Kroll, a global leader in risk mitigation. Over the past 14 years, Kroll has provided data breach response services for cases impacting more than 100 million individuals including personal consultation to more than 180,000 consumers and worked some 8,000 confirmed identity theft cases. When you need assistance, rest assured that your services are backed by an expert team who can answer any question you may have.

The following services are included in your **Credit Monitoring** package:

Kroll employs a team of experienced licensed investigators to provide you with expert, one-on-one assistance:

Consultation: You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes best practice tips to assist in ongoing protection, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Restoration: Kroll's restoration services are the most comprehensive of any provider. Should you become a victim of identity theft, a dedicated licensed investigator can work on your behalf to resolve related issues. The investigator does more than shoulder the bulk of the recovery; they can dig deep to uncover all aspects of the theft, and then work with creditors, collection agencies, utilities, government entities, and more ... to resolve it.

Credit Monitoring: Credit monitoring can be a key tool in detecting early warning signs of identity theft. You'll receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll investigator, who can help you determine if it's an indicator of identity theft. You'll also receive "no activity" notices if there have been no changes to your data.

Web Watcher: Web Watcher helps to detect if your personal information is being bought and sold online. This program monitors hacker chat rooms, forums and other websites where criminals are known to trade stolen information. Thousands of sites are monitored, looking for matches to your personal information, such as Social Security, medical ID, and financial account numbers. If your information is found, you will be promptly alerted and provided with instructions to contact your investigator. Monitoring starts as soon as you enroll and select the information to search.

How to Take Advantage of Your Identity Theft Protection Services

Visit kroll.idMonitoringService.com and follow the online instructions to take advantage of your identity theft protection services.

You can view your services at any time by logging onto Kroll's identity protection website. When you enroll, be prepared to provide the membership number included with the accompanying letter.

Help is only a phone call away.

If you have a question, need assistance, or feel you may be a victim of identity theft, call Kroll at the toll-free number provided in the accompanying letter, and ask to speak with an investigator.

Take advantage of this no-cost opportunity and let the experts at Kroll help you assess your situation and safeguard your identity.

Kroll.idMonitoringService.com is compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox or Safari.

State Notification Requirements

All States.
You may obtain a copy of your credit report or request information on how to place a fraud alert or security freeze by contacting any of the national credit bureaus below. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

For residents of Massachusetts.
It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of Massachusetts and West Virginia.
You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze and free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

For residents of Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, and West Virginia.
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

For residents of Iowa.
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon.
State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Illinois, Maryland and North Carolina.
You can obtain information from the Federal Trade Commission, and for residents of Maryland and North Carolina, from your respective state Office of the Attorney General, about steps you can take toward preventing identity theft.

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

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Barbecue Renew, Inc.:
FAQs concerning data breach and system intrusion at www.GrillParts.com

FAQs

How did Barbecue Renew first find out about the incident?

In October 2014, we received a Common Point of Purchase ("CPP") notification from payment card industry contacts informing us of at least two incidents of suspicious and potentially fraudulent activity originating from a number of payment cards used to purchase products through our website www.grillparts.com.

How did Barbecue Renew respond to the incident?

Following the initial CPP notification in October 2014, we immediately began working with our payment industry contacts and initiated an internal investigation to identify corrective measures and remediate any possible vulnerability that could have been exploited by attackers thereby resulting in a security breach. By October 21, 2014 we had remedied the vulnerability that was the suspected point of exploitation. Unfortunately, we received a CPP notification on Wednesday, November 12th, 2014 alerting of us of a third instance of suspicious and potentially fraudulent activity. Immediately thereafter, we launched an investigation and engaged leading IT security firms and forensic investigators, law enforcement and payment card industry contacts to ascertain the facts.

What information was exposed?

To date our investigation has confirmed a data breach resulting in potential risk and exposure of cardholder data, including cardholder names and addresses and payment card numbers, expiration dates and security codes. Our investigation is on-going and we will update as we are able to do so.

Is Barbecue Renew working with law enforcement?

We have contacted state law enforcement about this matter and will be actively cooperating with them.

How do I know if my credit card information has been compromised as a result of this incident?

We are working with leading IT security firms, forensic investigators, law enforcement and payment industry contacts to determine all of the facts and will share additional facts as they become available. We know that card holder information was potentially compromised as a result of the cyber attack. If you have received a copy of the notification letter, you should review it closely as it contains important information about steps you make take to protect yourself in the event your personal financial information has been compromised. If you have specific questions related to the security of your card holder information in light of this notification you should contact your card issuing bank directly.

Will I be responsible for fraudulent charges to the payment cards I used complete transactions through www.grillparts.com?

No. Customers will not be responsible for any fraudulent charges to their accounts – any fraudulent charges will be the responsibility of either Barbecue Renew or the bank that issued the card.

What should customers do?

It is always a good idea to regularly monitor card accounts and to quickly report suspicious activity to your card issuers. You can also take advantage of the programs described in your notification letter. For more information on monitoring credit cards and suspicious activity please call the number listed above.

How do I know if I am an impacted customer?

We will provide further information regarding who has been impacted as it becomes available, but if you have received a notification letter you should rely on the instructions we have provided in this communication

Why wasn't I notified sooner?

Barbecue Renew immediately launched an investigation into the incident following notification. The investigation included a review of internal security systems to confirm that procedures already in place are strengthened to further safeguard against a breach of data security in the future. Last, it was imperative that impacted individuals were identified and their contact information gathered into a consistent format for notification. This investigation was a time-consuming process, but we believed it was necessary to ensure appropriate precautions and next steps, such as notifying affected customers, were taken.