



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

STATE OF NH
DEPT. OF JUSTICE

2018 DEC 26 A 11: 05

Jeffrey J. Boogay
Office: 267-930-4784
Fax: 267-930-4771
Email: jboogay@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

December 21, 2018

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent Benchmade Knife Co., Inc. ("Benchmade"), located at 300 Beaver Creek Road, Oregon City, OR 97045. We are writing to notify your office of an incident that may affect the security of personal information relating to nine (9) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Benchmade does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about October 10, 2018, Benchmade began investigating suspicious activity occurring on their website, www.benchmade.com. Benchmade immediately shut down its website and began remediation efforts. Benchmade worked with third-party forensic investigators to determine the nature and scope of the event. On November 9, 2018, the investigation determined that an unauthorized party was able to obtain Benchmade customer payment card information entered between September 1, 2018, and October 10, 2018. This may include customers who completed online purchases and those who began transactions but did not complete the sale.

Benchmade next took steps to confirm the identities of the customers whose personally identifiable information was potentially impacted. On or around November 28, 2018, Benchmade confirmed the identities of the individuals who completed online transactions.

Since the event was discovered, Benchmade has been working with third-party forensic investigators to determine what happened, what information was potentially affected and to implement additional

procedures to further protect the security of customer debit and credit cards. Customers can safely use their payment cards on Benchmade's website.

The information that could have been subject to unauthorized access includes cardholder name, address, credit card number, expiration date, and CVV.

Notice to New Hampshire Residents

On or about December 21, 2018, Benchmade provided written notice of this incident to all affected individuals, which includes nine (9) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*. In addition to written notice to impacted individuals, Benchmade is issuing a press release to prominent media outlets serving New Hampshire and by conspicuously posting notice on their website. The press release issued by Benchmade relating to this matter is attached hereto as *Exhibit B*. The website notice issued by Benchmade relating to this matter is attached hereto as *Exhibit C*.

Other Steps Taken and To Be Taken

Upon discovering the event, Benchmade moved quickly to investigate and respond to the incident, assess the security of Benchmade systems, and notify potentially affected individuals. Benchmade is also working to implement additional safeguards and training to its employees.

Additionally, Benchmade is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Benchmade is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Benchmade is also providing written notice of this incident to other state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4784.

Very truly yours,



Jeffrey J. Boogay of
MULLEN COUGHLIN LLC

JJB:emp
Enclosure

EXHIBIT A



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>>

Re: Notice of Data Breach

Dear <<Name 1>>:

Benchmade Knife Co., Inc. (“Benchmade”), is writing to inform you of a recent event that may impact the privacy of some of your payment information. We wanted to provide you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On October 10, 2018, Benchmade began investigating suspicious activity occurring on their website, www.benchmade.com. Benchmade immediately launched an investigation and began working with third-party forensic investigators to determine the nature and scope of the event. On November 9, 2018, the investigation determined that an unauthorized party was able to obtain Benchmade customer payment card information entered between September 1, 2018, and October 10, 2018. This incident may affect customers who completed online purchases and those who began transactions but did not complete the sale.

Benchmade next took steps to confirm the identities of customers whose payment card information was impacted. On or around November 28, 2018, we confirmed the identities of the individuals who completed online transactions.

Since the event was discovered, we have been working with third-party forensic investigators to determine what happened, what information was potentially affected and to implement additional procedures to further protect the security of customer information. You can safely use your payment card at our website.

What Information Was Involved? Through the ongoing third-party forensic investigation, we confirmed on November 9, 2018, that unauthorized parties were able to obtain credit or debit card data from some transactions initiated at www.benchmade.com between September 1, 2018, and October 10, 2018. The information at risk as a result of the event includes the cardholder’s name, address, credit card number, expiration date, and CVV.

What We Are Doing. We take this incident and the security of your information very seriously. Upon learning of this incident, we immediately shut down our website and eliminated the source of the unauthorized access. As part of our ongoing commitment to the privacy of personal information in our care, we are continuing to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. We also notified state regulators, as required.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Prevent Fraud and Identity Theft*. We encourage you to remain vigilant against incidents of fraud by reviewing your account statements regularly and keeping a close eye on your credit card activity. If you see any suspicious activity, please report it to the bank that issued your credit card. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-877-565-6275, between the hours of 6:00 a.m. to 6:00 p.m. You may also write to Benchmade Knife Co., Inc., at 300 Beaver Creek Road, Oregon City, OR 97045.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

A handwritten signature in black ink, appearing to read "Mike Ulwelling". The signature is fluid and cursive, with a large, stylized "M" and "U".

Mike Ulwelling
Vice President of Marketing & Sales
Benchmade Knife Co., Inc.

STEPS YOU CAN TAKE TO BETTER PROTECT YOUR INFORMATION

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the 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. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872

www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order 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 (5) 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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 8 Rhode Island residents impacted by this incident.

EXHIBIT B

Benchmade Knife Co., Inc., Provides Notice of Data Security Incident

Oregon City, Oregon, December 21, 2018 – Benchmade Knife Co., Inc. (“Benchmade”), today announced that a recent data security incident may have resulted in unauthorized access to payment information of some customers who entered credit and debit cards on its website between September 1, 2018, and October 10, 2018. We engaged professionals who have corrected the issue and customers can now safely use their credit and debit cards at our website.

On October 10, 2018, Benchmade began investigating suspicious activity occurring on its website, www.benchmade.com. Benchmade immediately shut down its website and began remediation efforts. Benchmade also immediately launched an investigation and began working with third-party forensic investigators to determine the nature and scope of the event. On November 9, 2018, the investigation determined that an unauthorized party was able to obtain Benchmade customer payment information entered between September 1, 2018, and October 10, 2018, including the cardholder’s name, address, credit card number, expiration date, and CVV. This may include customers who completed purchases on the website and those who began transactions but did not complete the sale.

Benchmade next took steps to confirm the identities of the customers whose personally identifiable information was impacted. The company is notifying potentially affected customers and providing them with guidance on how they can protect themselves from fraud or identity theft.

Benchmade established a dedicated assistance line for individuals seeking additional information regarding this incident. Customers can call 1-877-565-6275, Monday through Friday (excluding U.S. holidays), 6:00 a.m. to 6:00 p.m. EST. Customers can also find additional information on this incident and what they can do to better protect against fraud and identity theft at www.benchmade.com.

Benchmade takes this incident and the security of our customers’ information very seriously. The company has updated processes to further strengthen its systems to protect customer debit or credit card information and will continue to work with third-party experts to help ensure the highest levels of security.

###

EXHIBIT C

Benchmade Knife Co., Inc., Provides Notice of Data Security Incident

Oregon City, Oregon, December 21, 2018 – Benchmade Knife Co., Inc. (“Benchmade”), today announced that a recent data security incident may have resulted in unauthorized access to payment information of some customers who entered credit and debit cards on its website between September 1, 2018 and October 10, 2018. We engaged professionals who have corrected the issue and customers can now safely use their credit and debit cards at our website.

On October 10, 2018, Benchmade began investigating suspicious activity occurring on its website, www.benchmade.com. Benchmade immediately launched an investigation and began working with third-party forensic investigators to determine the nature and scope of the event. On November 9, 2018, the investigation determined that an unauthorized party was able to obtain Benchmade customer payment information between September 1, 2018, and October 10, 2018, including credit and debit card information used for online transactions initiated during this period. Specific information potentially accessed includes the cardholder’s name, address, credit card number, expiration date, and CVV. This may include customers who completed purchases on the e-commerce website and those who began transactions but did not complete the sale.

Benchmade next took steps to confirm the identities of the customers whose personally identifiable information was impacted. The company is notifying potentially affected customers by mail, this posting, and by notifying the media about this event. Potentially affected customers can review the information below for steps on how they can protect themselves from fraud or identity theft.

Benchmade established a dedicated assistance line for individuals seeking additional information regarding this incident. Customers can call 1-877-565-6275, Monday through Friday (excluding U.S. holidays), 6:00 a.m. to 6:00 p.m. EST. Customers can also find additional information below on how they can protect against fraud and identity theft.

Benchmade takes this incident and the security of our customers’ information very seriously. The company has updated processes to further strengthen its systems to protect customer debit or credit card information and will continue to work with third-party experts to help ensure the highest levels of security.

###

STEPS YOU CAN TAKE TO BETTER PROTECT YOUR INFORMATION

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. If you see any suspicious activity, please report it to the bank that issued your credit card. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the 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. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian PO Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion P.O. Box 2000 Chester, PA 19016 1-888-909-8872 www.transunion.com/credit-freeze	Equifax PO Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/credit-report-services
---	---	---

In order 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 (5) 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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	TransUnion P.O. Box 2000 Chester, PA 19106 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	Equifax P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services
---	---	--

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 8 Rhode Island residents impacted by this incident.