MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Sian M. Schafle
Office: (267) 930-4799
Fax: (267) 930-4771
Email: sschafle@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

January 16, 2020

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent the National Association of Manufactures ("NAM") located at 733 10th Street NW, #700, Washington, DC 20001 and are writing to notify your Office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, the NAM 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

The NAM became aware of unusual activity relating to certain NAM systems and promptly began an investigation with the assistance of computer forensic investigators. The investigation determined that information in certain employee email accounts may have been subject to unauthorized access between December 7, 2018 and April 29, 2019. The investigation was unable to determine which, if any, emails and attachments within the email accounts were accessed or viewed. Therefore, the NAM undertook a comprehensive review of the email accounts to determine whether they contained any sensitive information. Upon completion of this review, on December 10, 2019, the NAM confirmed that personal information as defined by N.H. Rev. Stat. § 359-C:19 was present within the relevant email accounts at the time of the incident. The information related to the New Hampshire resident include name and credit/debit card information. The NAM then moved quickly to notify the state resident.

Notice to New Hampshire Resident

On January 16, 2020, the NAM provided written notice of this incident to affected individuals, which includes one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, the NAM moved quickly to investigate and respond to the incident, assess the security of NAM systems, and notify potentially affected individuals. The response included reviewing the contents of the email account to determine whether they contained sensitive information, and reviewing internal systems to identify contact information for purposes of providing notice to potentially affected individuals. As part of the NAM's commitment to the security of information, the NAM is also reviewing and enhancing existing security policies and procedures and conducting additional workforce training to reduce the likelihood of a similar future event.

The NAM is providing access to credit monitoring services for one (1) year, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Additionally, the NAM 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. The NAM is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, 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. The NAM is notifying relevant state regulators and will cooperate with any law enforcement investigation relating to this incident.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4799.

Very truly yours,

Sian M Schafle.

Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS/mep

Exhibit A

NATIONAL ASSOCIATION OF
Manufacturers

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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

The National Association of Manufacturers ("NAM") writes to notify you of an incident that may affect the privacy of some of your personal information. While, to date, we are unsure whether your information was actually viewed and have no evidence of actual or attempted misuse of your personal information as a result of this incident, this letter provides details of the incident, our response, and resources available to you to help protect your personal information from possible misuse, should you feel it is appropriate to do so.

What Happened? The NAM became aware of unusual activity relating to certain NAM systems and promptly began an investigation with the assistance of computer forensic investigators. The investigation determined that information in certain employee email accounts may have been subject to unauthorized access between December 7, 2018 and April 29, 2019. The investigation was unable to determine which, if any, emails and attachments within the email accounts were accessed or viewed. Therefore, the NAM undertook a comprehensive review of the email accounts to determine whether they contained any sensitive information. On December 10, 2019, the review determined that some of your personal information was present in an involved email account at the time of the incident.

What Information Was Involved? The investigation determined that your <<ClientDef1(Impacted Data)>> were present in an involved email account at the time of the incident. To date, we are unaware of any actual or attempted misuse of your personal information and in fact do not know whether there was any attempt to view your personal information. We know only that your personal information was present in an involved email account.

What Are We Doing. The security of the information in our systems is among our highest priorities, and we have security measures in place to protect information in our care. Upon learning of this incident, we moved quickly to investigate and respond to this incident, assess the security of relevant NAM systems, and notify potentially affected individuals. Our response included resetting relevant passwords, reviewing the contents of the email accounts to determine whether they contained sensitive information, and reviewing internal systems to identify contact information for purposes of providing notice to potentially affected individuals. As part of our ongoing commitment to the security of information, we are also reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.

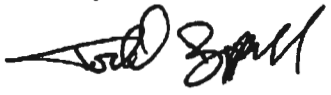
The NAM notified relevant state regulators. Law enforcement is also aware of this incident and the NAM will cooperate with any law enforcement investigation. In an abundance of caution we are notifying you of this event and providing you access to identity monitoring services through Kroll for 12 months at no cost to you. While the NAM will cover the costs of these services, you will need to complete the activation process.

What Can You Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to monitor your account statements and credit reports for suspicious activity. You may also review the information contained in the attached "Steps You Can Take to Help Safeguard Your Information" for additional information on how you can monitor your identity and on how to activate the free identity monitoring services.

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-866-775-4209 (toll free), Monday through Friday, 9:00 a.m. to 6:30 p.m., ET. You may also write to us at 733 10th St. NW #700, Washington, DC 20001.

We regret any inconvenience this incident may cause you. The NAM remains committed to safeguarding information in our care, and we will continue to take proactive steps to enhance the security of our systems.

Sincerely,



Todd Boppell
Chief Operating Officer
National Association of Manufacturers

Steps You Can Take to Help Safeguard Your Information

Activate Your Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring 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 monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.
*You have until **April 15, 2020** to activate your identity monitoring services.*
Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

Monitor Accounts

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	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 160	PO Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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 1-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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

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 Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

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, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

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 violators. 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 New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will 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 fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, 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.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
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.