MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

James E. Prendergast
Office: 267-930-4798
Fax: 267-930-4771
Email: jprendergast@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

June 4, 2019

VIA U.S. MAIL

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

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent The LKQ Corporation ("LKQ"), 655 Grassmere Park Nashville, TN 37211 and are writing to notify you of a recent incident that may affect the security of the personal information of certain New Hampshire residents. The investigation into this event is ongoing, and this notice may be supplemented if significant facts learned subsequent to its submission. By providing this notice, LKQ does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Security Incident

LKQ recently became aware of a pattern of suspicious activity relating to an LKQ employee email account. In response, a privileged third-party forensic investigation was conducted to determine the nature and scope of the activity. The investigation determined that the email account was accessed without authorization between October 31, 2018 and January 9, 2019. Every potentially accessible file within the impacted account was reviewed to determine what files may have been accessible to the unauthorized actor. On April 23, 2019 LKQ identified the names of individuals whose information was included in the potentially accessible files. LKQ continued to work to obtain contact information for impacted individuals through May 31, 2019. Through this review, LKQ determined that personal information relating to two (2) New Hampshire residents was potentially affected.

While the types of personal information impacted may vary by individual, the investigation determined the names and financial account information and routing numbers relating to two (2) New Hampshire residents, were impacted in relation to this incident.

Notice to New Hampshire Residents

LKQ provided written notice of this incident to two (2) New Hampshire residents on June 4, 2019, in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

The confidentiality, privacy, and security of personal information is among LKQ's highest priorities. Upon learning of the event, LKQ investigated to determine those individuals that were affected, and secured the compromised accounts by updating passwords. LKQ will be taking additional steps to improve security and better protect against similar incidents in the future.

LKQ is providing potentially affected individuals access to 12 months of credit monitoring and identity restoration services through Epiq. Additionally, LKQ is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including 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 identity theft and fraud 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security incident, please contact me at (267) 930-4798.

Very truly yours,

Jim Prendergast of
MULLEN COUGHLIN LLC

EXHIBIT A

[LKQ Letterhead/Logo]

[redacted]

Re: Notice of Data Breach

Dear [redacted]:

LKQ Corporation ("LKQ") is writing to notify you of a recent incident that may have impacted the security of your personal information. We want to provide you with information about the incident, our response, and steps you may take to better protect against possible misuse of your personal information, should you feel it necessary to do so.

What Happened? LKQ recently became aware of a pattern of suspicious activity relating to an LKQ employee email account. In response, LKQ worked with an outside forensics expert to investigate the nature and scope of the activity. The investigation determined that the email account was accessed without authorization between October 31, 2018 and January 9, 2019. Every potentially accessible file within the impacted accounts was reviewed to determine what files may have been accessible to the unauthorized actor. We have determined that your information was included in the potentially accessible files.

What Information was Involved? The investigation determined that your name, address and details for your bank account ending in [redacted] were accessible by the unauthorized actor. Specifically, this information was included in a residential property purchase and sales agreement for the purchase of property at the above listed address. It appears that this information was unrelated to LKQ but, rather, was related to an LKQ employee's personal activities. While this information was accessible, there is no indication that this information was actually viewed by the unauthorized actor.

What We Are Doing. The confidentiality, privacy, and security of personal information within our care is among LKQ's highest priorities. Upon learning of the event, we investigated to determine those individuals that were affected and secured the compromised accounts by updating passwords. We will be taking additional steps to improve security and better protect against similar incidents in the future.

What You Can Do. Please review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud*, which contains information on what you can do to better protect against possible misuse of your information.

As an added precaution, LKQ is offering you access to an online credit monitoring service (myTrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the myTrueIdentity website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code [redacted] and follow the three steps to receive your credit monitoring service online within minutes.

You can sign up for the online credit monitoring service anytime between now and September 30, 2019. Due to privacy laws, we cannot register you directly. Please note that credit monitoring service might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

If you believe you may be a victim of identity theft, please call the toll-free TransUnion Fraud Response Services hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code [redacted] to speak to a TransUnion representative about your identity theft issue.

For More Information. You may have questions that are not answered in this letter. If you have questions please call Julie A. Inderlied, CPO and Senior Compliance Counsel (678-230-0138).

Sincerely,

Vic's signature block
SIGNATURE

NAME
TITLE

Steps You Can Take to Protect Against Identity Theft and Fraud

In addition to enrolling in the above offered services, 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 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	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
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.