BARNES & THORNBURG LLP

11 S. Meridian Street
Indianapolis, IN 46204-3535 U.S.A.
(317) 236-1313
Fax (317) 231-7433

www.btlaw.com

Todd G. Vare
Partner
(317) 231-7735
Todd.Vare@btlaw.com

March 9, 2020

VIA EMAIL

To:

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
Email: consumer@ag.iowa.gov

Re: Security Event Notice Provided for Gurley-Leep Automotive Management Corporation

To whom it may concern:

Barnes & Thornburg LLP acts as attorneys for the Gurley-Leep Automotive Management Corporation ("Gurley Leep"), an entity incorporated in the State of Indiana and located at 5201 North Grape Road, Mishawaka, Indiana, 46545, with respect to a data security event and the exposure of certain personal information as described in more detail below.

1. Nature of the Security Event

On April 24, 2019, unknown cyber criminals launched a sophisticated ransomware attack, which disabled various computer systems across the company. Based on the results of Gurley Leep's investigation both internally and with an outside third party forensics investigator, a good faith determination was reached that notification would not be required.

Subsequently, on January 24, 2020, the existence of an additional document possibly containing personal information of various employees personally maintained by one individual employee was brought to the attention of Gurley Leep. The original document and its contents were and remain encrypted and inaccessible due to the ransomware attack.

At this time, the evidence available has not revealed any unauthorized access or misuse of personally identifying, sensitive information. Updated information will be provided by Gurley Leep if and when such information becomes available.

2. Number of Iowa Residents Affected

One-thousand six-hundred and twenty-four (1,624) of the affected individuals are residents of Iowa. The investigation continues in an attempt to discern the information contained within the document as well as the individuals for whom notification may be required. However, out of an abundance of caution, Gurley Leep intends to notify all past and current employees dating as far back as January 1, 2000. The document subject to the original ransomware attack is believed to have include names, addresses, social security numbers, and other financial information related to various Gurley Leep employees.

3. Steps Taken or Planned to be Taken Related to the Security Event

The following remedial steps have been taken in response to the April 24, 2019, ransomware attack:

Complete reimaging of all workstation computers across the company.
Cleaned up servers on network and removed encrypted data and remaining malware.
Implemented new security protocols to user email accounts.
Updated previous spam filter to Microsoft Office 365 Protection.
Migrated to Microsoft Azure AD Connect.
Two Factor Authentication implemented for all personal administrator logins.
Removed unnecessary servers and reorganized remaining servers.
Removed and replaced network firewall with recommended firewall.
Removed and replaced existing Anti-Virus software with recommended software.
Implemented new backup solution.
Mandatory password reset for all users within the Gurley-Leep network.
Drafting of new Incident Response Plan.
Implementation of quarterly network testing by a third-party provider.

Gurley Leep is currently working with third-party service provider, Experian, to draft and finalize the breach notification letter to be sent to affected employees. A copy of the breach notification will provide it once it becomes available.

4. Contact Information

Please contact the undersigned with any questions regarding this incident.

Very truly yours,

BARNES & THORNBURG LLP

Todd G. Vare

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

April 1, 2020

F4427-L01-0000001 P001 T00001 **********MIXED AADC 159
SAMPLE A SAMPLE - L01 GENERAL
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

NOTICE OF DATA SECURITY INCIDENT

Dear Sample A Sample:

We are writing to inform you of a recent data security incident that has the potential to impact our current and previous employees. Although at this time we are not aware of any misuse of your information, we are providing this notice to ensure that you may take steps to protect your information should you feel it is appropriate to do so.

WHAT HAPPENED?

On April 24, 2019, the cyber criminals launched a sophisticated ransomware attack, which disabled various computer systems across the company. Due to the nature and effects of the ransomware attack, the exact scope of the security incident and the unauthorized actors' access to our network is indeterminable. Our in-depth cybersecurity forensics review of the evidence available has not revealed any unauthorized access or misuse of personally identifying, sensitive information. However, due to the limited nature of the evidence available, the possibility of unauthorized access cannot, at this time, be definitively ruled out. We are contacting you to provide you with further information and resources relating to this attack.

WHAT INFORMATION MAY HAVE BEEN INVOLVED?

Due to the nature of the ransomware attack, and despite our investigation, we are unable to determine exactly what information the attackers may have accessed and therefore must presume the attackers may have accessed and/or duplicated any of the information available within Gurley Leep's corporate network. This information includes names, current and/or past addresses, social security numbers, birthdates, employee benefits information, and email addresses.

WHAT WE ARE DOING

Upon learning of the incident, Gurley Leep engaged outside counsel and forensic investigators to perform and assist with our investigation into the attack. Additionally, Gurley Leep has taken various steps to neutralize the existing threat and has implemented additional security measures designed to remove the cyber criminals' access to our systems and to detect and prevent future threats. Our current investigation has not yielded any evidence of additional existing threats and we will continue to carefully monitor for signs of further activity or compromise. We are also providing resources, explained in this letter, to help protect against potential misuse of your information.

WHAT YOU CAN DO

Please review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information.

Additionally, we have arranged for you, at your option, to enroll in Experian's® IdentityWorksSM, a complimentary service providing you identity detection and resolution of identity theft. This service provides: (i) daily credit monitoring of your Equifax, Experian and TransUnion credit files, (ii) unlimited access to your Equifax Credit Report, (iii) an annual 3-in-1 Credit Report which provides you with your credit history as reported by the three major credit reporting agencies, (iv) the ability to lock and unlock your Equifax credit file in real time, (v) the ability to set a fraud alert on your credit file at all 3 bureaus and automatically renew every 90 days, (vi) scans of the internet for your personal information and alerts if it is found on suspected underground trading sites, (vii) wallet replacement assistance in the event of a lost/stolen wallet, and (viii) identity theft insurance up to $1,000,000 to cover certain out of pocket expenses arising from an occurrence of identity theft, subject to certain limitations and exclusions. You have until MM/DD/YYYY (your activation code will not work after this date), to activate the free, optional service by using the following activation code: ABCDEFGHI. This code is unique for your use and should not be shared. Please go to https://www.experianidworks.com/credit to enroll or call 1-855-223-4413 for assistance. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the identity restoration services by Experian.

FOR MORE INFORMATION

If you have questions not addressed by this letter, please do not hesitate to contact the call center we have established at 1-855-223-4413 between 9:00 a.m. - 9:00 p.m. EST from Monday through Friday and 11 a.m. – 8 p.m. Saturday through Sunday.

Sincerely,

Chris Pustelak
Vice President of Operations

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

1) Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

You should always remain vigilant for incidents of fraud and identity theft. Over the next twelve to twenty four months, we recommend that you remain especially vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Obtain and Monitor Your Credit Report
We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at: https://www.annualcreditreport.com/requestReport/requestForm.action.

Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies, for the purpose of requesting a copy of your credit report or for general inquiries, is provided below:

Equifax (866) 349-5191 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian (888) 397-3742 www.experian.com P.O. Box 4500 Allen, TX 75013	TransUnion (800) 888-4213 www.transunion.com 2 Baldwin Place P.O. Box 1000 Chester, PA 19016

2) Consider Placing a Fraud Alert on Your Credit Report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

3) Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information.

Additional information is available at:
https://www.consumer.ftc.gov/topics/privacy-identity-online-security.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338).

A copy of *Identity Theft – A Recovery Plan*, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

You may also wish you review information provided by your local Attorney General's Office at https://www.website.gov/sample/, by calling #-###-###-####, or by writing to Sample Government Center, 123 Sample St, 1st Floor, Anytown, US 12345.

4) Security Freeze

In all US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.

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	1-800-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services/

5) MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with, and shredding receipts, statements, and other sensitive information.

6) USE TOOLS FROM CREDIT PROVIDERS

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.