BakerHostetler

Baker&Hostetler LLP

Key Tower
127 Public Square, Suite 2000
Cleveland, OH 44114-1214

T 216.621.0200
F 216.696.0740
www.bakerlaw.com

David E. Kitchen
direct dial: 216.861.7060
dkitchen@bakerlaw.com

February 19, 2021

VIA E-MAIL (CONSUMER@AG.IOWA.GOV)

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, IWI Motor Parts ("IWI"), to notify you of a security incident involving Iowa residents. IWI is a company in the automotive aftermarket business. IWI is headquartered in Dubuque, IA and also has operations in Illinois and Wisconsin.

IWI has conducted an investigation involving unauthorized access to some of its company servers. That investigation determined that the access occurred on October 31, 2020. Upon discovering the incident, IWI immediately took steps to secure its systems and launched an investigation with the assistance of a professional security firm to determine the nature and scope of the incident. IWI's investigation determined that an unauthorized person accessed certain files on its servers and transferred at least some of those files outside of the network. On January 27, 2021**,** IWI determined that the files accessed and/or transferred out of its network by the unauthorized person contained information pertaining to certain individuals. On February 12, 2021, IWI determined that the information of 656 Iowa residents may have been accessed, including their names and one or more of the following: Social Security number and/or financial account number.

Beginning today, February 19, 2021, IWI is providing written notice to the Iowa residents via First Class U.S. Mail. A sample copy of the notification letter is enclosed. IWI is offering the Iowa residents whose Social Security numbers were involved a complimentary one-year membership in credit monitoring and identity theft protection services through Kroll. IWI has also

established a dedicated call center where all individuals may obtain more information regarding the incident.

To further protect personal information, IWI continues to review its systems and has implemented addition measures to further enhance and strengthen its existing security processes.

Please do not hesitate to contact me if you have any questions regarding this incident.

Sincerely,

David E. Kitchen
Partner

Enclosure

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

At IWI Motor Parts, we understand the importance of protecting and securing the information we maintain. We are writing to inform you of an incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you may consider taking.

On December 6, 2020, we identified a security incident involving ransomware. We immediately took steps to secure and restore our network and began an investigation with the assistance of a cybersecurity firm to determine the nature and scope of any unauthorized access. We also implemented additional measures to further enhance the security of our network.

The investigation determined that an unauthorized person had accessed our systems beginning on October 31, 2020, during which time they accessed certain files. We carefully reviewed the files that were accessed and, on January 27, 2021, determined that one of the files contained your <<b2b_text_1(ImpactedData)>>.

Although we have no indication that your information has been misused, we wanted to notify you of this incident and assure you that we take it very seriously. We encourage you to remain vigilant by regularly reviewing your financial account statements for any unauthorized activity. If you see charges or activity you did not authorize, please contact your financial institution immediately. As an added precaution, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. For more information on Kroll Identity Monitoring, including instructions on how to activate your complimentary one-year membership, please visit the below website:

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.
*You have until **May 20, 2021** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

Your confidence and trust are important to us, and we regret any inconvenience or concern this incident may cause. To further protect personal information, we continue to review our systems and have implemented additional measures to further enhance and strengthen our existing security processes. If you have any questions, please call 1-XXX-XXX-XXXX, Monday through Friday from 8:00 A.M. through 5:30 P.M. Central Time.

Sincerely,

TJ Faley
President

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is 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 will be able to 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.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov