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 5, 2021

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, Tom Wood Group ("TWG"), to notify you of a data security incident involving three New Hampshire residents.[1] TWG is an owner and operator of car dealerships and leasing agencies based in Indianapolis, Indiana.

On October 19, 2020, TWG identified a security incident that resulted in the encryption of certain systems within its environment. TWG immediately began an internal investigation, a cybersecurity firm was engaged, and steps were taken to address the incident and restore operations. The investigation determined that an unauthorized person obtained access to TWG's systems between October 5, 2020 and October 19, 2020 and acquired a limited amount of information that is maintained on TWG's systems. On January 1, 2021, TWG completed a review of those files and determined that the files contained certain information pertaining to individuals, three of whom were subsequently determined to be New Hampshire residents, including the residents' names with one or more of the following data elements: Social Security numbers and/or driver's license numbers.

Beginning today, TWG is providing written notification letters to the New Hampshire residents via U.S. mail. A sample copy of the notification letter is enclosed. TWG is offering the three New Hampshire residents a one-year membership in complimentary credit monitoring, fraud consultation, and identity theft restoration services through Kroll. TWG has also established a

[1] This notice does not waive TWG's objection that New Hampshire lacks personal jurisdiction over it regarding any claims related to this data security incident.

dedicated call center that individuals may call with related questions and provide individuals with other steps they can take to protect their information.

To reduce the risk of a similar incident occurring in the future, TWG reset all network account passwords and has implemented additional safeguards and technical security measures, such as multi-factor authentication for all network accounts, restricted network access, and new security software, to further protect personal information. TWG is also engaging a third-party consultant to assist with security enhancements, enhancing internal policies and procedures, installing anti-phishing software, and requiring its employees to participate in additional internet safety training.

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

Sincerely,

David E. Kitchen
Partner

Enclosure

TOM WOOD GROUP

<<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>>,

Tom Wood Group ("TWG") is committed to protecting the privacy of information we maintain. We are contacting you because we recently addressed an incident that may have involved some of your information. This notice describes the incident, measures we have taken, and some steps that you may consider taking in response.

TWG identified a security incident on October 19, 2020 that resulted in the encryption of certain systems within our environment. We immediately began to investigate, a cybersecurity firm was engaged, and steps were taken to address the incident and restore operations. Through our investigation, we determined that an unauthorized person obtained access to our systems between October 5, 2020 and October 19, 2020, and acquired a limited amount of information that was maintained on our systems. On January 1, 2021, we completed a review of the files that may have been acquired and determined that they contained some of your information, including your <<b2b_text_1(ImpactedData)>>.

While we have no indication that your information was actually viewed by the unauthorized person, or that it has been misused, we wanted to notify you of this incident and assure you that we take it very seriously. Out of an abundance of caution, 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 identity theft prevention and 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 6, 2021** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

Your confidence and trust are important to us, and we sincerely regret that this incident occurred and apologize for any inconvenience or concern. To help prevent something like this from happening again, we have implemented additional safeguards and technical security measures, such as multi-factor authentication, to further protect employee data. We have also engaged a third-party consultant to provide security training to our employees.

If you have any questions, please call 1-833-960-3584, Monday through Friday, between 9:00am and 6:30pm Eastern Time.

Sincerely,

John Wood
Vice President

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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.

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

If your health insurance or medical information was involved, it is also advisable to review the billing statements you receive from your health insurer or healthcare provider. If you see charges for services you did not receive, please contact the insurer or provider immediately.

If your username and password to an online account was involved, it is also advisable to change your password to the account as well as any other accounts that use the same or a similar password.

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

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.