



David McMillan, Partner
Cybersecurity & Data Privacy Team
175 Pearl Street, Suite C-402
Brooklyn, NY 11201
dmcmillan@constangy.com
Mobile: 718.614.8371

September 26, 2024

VIA EMAIL

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP, represents Bay Ridge Automotive Management Group (“BRAM”) in connection with a recent data security incident described in greater detail below. This notice is being sent because personal information for Maryland residents may have been involved in the incident. The purpose of this letter is to notify you of the incident in accordance with Maryland’s data breach notification statute Md. Code Ann., Com. Law § 14-3501 et seq.

1. Nature of the Security Incident

On February 2, 2024, BRAM became aware of unusual network activity and immediately took steps to secure its systems. BRAM engaged cybersecurity experts to assist with the process. The investigation determined that certain data stored within the BRAM network may have been acquired without authorization on or about February 2, 2024. As a result, BRAM undertook a review of the potentially affected files. That review concluded on August 29, 2024 and revealed individuals whose personal information may have been affected.

2. Number of Maryland Residents Involved

Beginning September 26, 2024, BRAM notified 11 Maryland residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

The personal information involved in this incident includes individuals’ names, Social Security number, and driver's license number.

Page 2

3. Steps Taken to Address the Incident

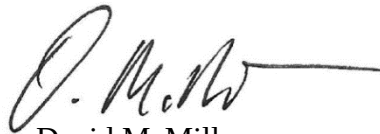
As soon as BRAM discovered this unusual network activity, it took steps to secure the affected systems and launched an investigation to determine whether, and to what extent, personal information had been accessed or acquired without authorization. BRAM has also implemented additional security measures in an effort to prevent a similar incident from occurring in the future. Further, as referenced in the sample consumer notification letter, the BRAM has offered individuals 12 months of complimentary services through IDX, which include Credit Monitoring, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

BRAM has established a toll-free call center through IDX to answer questions about the incident and address related concerns.

4. Contact Information

BRAM remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at dmcmillan@constangy.com

Sincerely,

A handwritten signature in black ink, appearing to read "D. McMillan", followed by a horizontal line extending to the right.

David McMillan
Partner, Cybersecurity & Data Privacy Team

Enclosure: Sample Notification Letter

BRAM

AUTO GROUP

Return Mail Processing Center:
PO Box 480149
Niles, IL 60714

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip Code>>

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

September 26, 2024

Subject: Notice of Data <<Breach/Security Incident>>

Dear <<First Name>> <<Last Name>>:

Bay Ridge Automotive Management Group (“BRAM”) writes to notify you regarding a data security incident that may have affected the privacy of your information. BRAM takes this incident seriously and is providing you with information about the incident, our response, and steps you can take to help protect your information.

What Happened. On February 2, 2024, BRAM became aware of unusual network activity and immediately took steps to secure our systems. We engaged cybersecurity experts to assist with the process. The investigation determined that certain data stored within our network may have been acquired without authorization on or about February 2, 2024. As a result, BRAM undertook a review of the potentially affected files. Our review concluded on August 29, 2024, and identified that some of your information may have been involved.

What Information Was Involved. The potentially affected information may have included your name as well as your <<Breached Elements>>.

What We Are Doing. As soon as BRAM discovered the incident, we took the steps described above and implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future.

In addition, we are offering you the opportunity to enroll in complimentary credit monitoring and identity theft protection services through IDX, A ZeroFox Company, a data breach and recovery services expert. IDX identity protection services include: <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do: Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information. You can also enroll in the IDX identity protection services, which are offered to you at no cost, using the instructions above. Please note the deadline to enroll in these services is December 26, 2024.

For More Information. If you have questions about this letter or need assistance, please call IDX at 1-866-815-8424. IDX representatives are available Monday through Friday from 9:00 am – 9:00 pm Eastern Time. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

Bay Ridge Automotive Management Group
7500 Westside Avenue
North Bergen, NJ 07047

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain 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, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may 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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: 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 at least 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>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.

