MAYNARD
COOPER GALE

**J.T. Malatesta**
DIRECT 205.254.1180
EMAIL JMalatesta@maynardcooper.com

September 17, 2021



**Attorney General Gordon McDonald**
Office of Attorney General
33 Capitol Street
Concord, NH 03301

**Re: Notice of a Security Incident**

Dear Attorney General McDonald,

I am writing to let you know that our client, Club Car, LLC ("Club Car" or "the Company"), experienced a security incident that affected the personally identifiable information ("PII") of some employees and vendors, including one (1) individual in New Hampshire. We are providing notice to your office pursuant to N.H. Rev. Stat. § 359-C:19, *et seq.*

On July 12, 2021, Club Car detected suspicious activity on an email account belonging to one of its employees. The Company immediately notified law enforcement and also engaged outside experts to investigate the situation. The investigation revealed that an unauthorized party had accessed this account in an attempt to commit financial fraud against the Company. Thankfully, those efforts were not successful. However, our review of the impacted account also revealed that it contained files that referenced the personal information of some Company employees and vendors. These individuals were notified by mail on Friday, September 17, 2021. A copy of the notice is enclosed as Exhibit A.

Club Car is not aware of any actual or attempted misuse of personal information as a result of this incident. Club Car is strengthening its email security by disabling legacy authentication, creating conditional access rules, and implementing multi-factor authentication. The Company will also continue to prioritize cybersecurity awareness training with its users.

Please do not hesitate to let me know if you have any questions or would like additional information.

Sincerely,

J.T. Malatesta

Enclosure

**Club Car, LLC**
4125 Washington Road
Evans, Georgia 30809
PO Box 204658
Augusta Georgia 30917
Tel (706) 863-3000
Toll free (800) 227-0739
Fax: (706) 228-2778
www.ClubCar.com

September 17, 2021

**VIA US MAIL**
SAMPLE A

**Re: Notice of Security Incident**

Dear [Name],

We hope this letter finds you well. We are writing to let you know about a security incident at Club Car that involved the personal information we have on file for you. We are not aware of any actual or attempted misuse of your personal information as a result of this incident. However, we want to make sure that you are aware of what happened so that you can take the appropriate precautions you feel are needed to protect your identity. We have enclosed information on several identity protection resources.

**What Happened?**
On July 12, 2021 we detected suspicious activity on an email account belonging to one of our employees. We immediately notified law enforcement, and began working with outside experts to investigate the situation. From our investigation, we determined that an unauthorized third party had accessed this email account in an attempt to commit financial fraud against our company. Thankfully, those efforts were unsuccessful. However, our experts reported that your personal information would have been available within documents maintained in this email account.

**What Information Was Available?**
The e-mail account contained documents that referenced your individual name and social security number.

**What We Are Doing**
We are committed to protecting the information we maintain here at Club Car. The referenced e-mail account has been secured, and we will continue to focus on strengthening the cyber-resiliency and security posture of our company.

**What You Can Do**
The enclosed Identity Protection Reference Guide includes information on general steps you can take to monitor and protect your personal information. We would encourage you to review these materials, and take the appropriate steps you feel are warranted. We are also offering one year of complimentary credit monitoring and identity protection services. If you would like to enroll in this service please reach out to Sandy Sullivan at sandy.sullivan@clubcar.com. Sandy is also available to answer any questions you may have about this notice.

We are sorry this happened, and for any inconvenience this may cause you.

Sincerely,

John Ansted
Vice President of Human Resources

## IDENTITY PROTECTION REFERENCE GUIDE

**1. Review your Credit Reports.** Monitor your credit reports for any activity you do not recognize. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To order your free annual credit report, visit www.annualcreditreport.com, call toll-free (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

If you see anything in your credit report that you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

**2. Place Fraud Alerts.** You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. Please note that placing a fraud alert may delay you when seeking to obtain credit. You can learn more about fraud alerts by contacting the credit bureaus or by visiting their websites:

| Equifax | Experian | TransUnion |
|---|---|---|
| 1-800-525-6285 | 1-888-397-3742 | 1-800-680-7289 |
| P.O. Box 740241 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30374-0241 | Allen, TX 75013 | Chester, PA 19022-2000 |
| www.equifax.com | www.experian.com | www.transunion.com |

It is only necessary to contact <u>one</u> of these bureaus and use only <u>one</u> of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You should receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

**3. Place Security Freezes.** By placing a security freeze, someone who fraudulently acquires your personally identifying information will not be able to use that information to open new accounts or borrow money in your name. Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze.

To place a security freeze, you must contact <u>each</u> of the three national credit reporting bureaus listed above and provide the following information: (1) your full name; (2) your social security number; (3) date of birth; (4) the addresses where you have lived over the past two years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail, the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus must send confirmation to you within five business days and provide you with information concerning the process by which you may remove or lift the security freeze.

**4. Monitor Your Account Statements.** We encourage you to carefully monitor your financial account statements, medical provider statements, and insurance statements for fraudulent activity and report anything suspicious to the respective institution or provider.

**5. You can obtain additional information** about the steps you can take to avoid identity theft and more information about fraud alerts and security freezes from the FTC. You may contact the FTC, Consumer Response Center at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502.

**********

**Iowa Residents:** You can report suspected identity theft to law enforcement, the FTC, or to the Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, 1-888-777-4590, https://www.iowaattorneygeneral.gov/.

**Massachusetts Residents:** You have a right to file a police report and obtain a copy of your records. You can obtain additional information about identity theft prevention and protection from the Office of Consumer Affairs and Business Regulation, 501 Boylston Street, Suite 5100, Boston, MA 02116, (617) 973-8787, https://www.mass.gov/service-details/identity-theft.

**North Carolina Residents:** You can obtain additional information about preventing identity theft from the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free within North Carolina) or (919) 716-6000, https://ncdoj.gov/.

**Oregon Residents:** You can report suspected identity theft to law enforcement, the FTC, or the Oregon Office of the Attorney General at: Oregon Department of Justice, 1162 Court St NE, Salem, OR 97301, 1-800-850-0228, https://www.doj.state.or.us/.