

Colin M. Battersby
Direct Dial: (248) 593-2952
E-mail: cbattersby@mcdonaldhopkins.com

June 11, 2024

VIA EMAIL (Idtheft@oag.state.md.us)

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Carolina Foods, LLC – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Carolina Foods, LLC (“Carolina Foods”). I am writing to provide notification of an incident at Carolina Foods that may affect the security of personal information of approximately one (1) Maryland resident for whom it had a last known home address. By providing this notice, Carolina Foods does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about March 12, 2024, Carolina Foods detected unauthorized access to their network environment. Upon learning of this issue, Carolina Foods immediately took steps to secure the threat and commenced a prompt and thorough investigation with external cybersecurity professionals experienced in handling these types of incidents. Following the conclusion of an extensive forensic investigation and thorough manual review, Carolina Foods determined on May 8, 2024 that certain files containing personal information was subject to unauthorized access and acquisition as a result of this incident, which potentially included affected resident’s full names, Social Security number, and one or more of the following, to the extent it is in their records: passport and or driver’s license.

To date, the Carolina Foods is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, Carolina Foods wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. Carolina Foods is providing the affected resident with written notification of this incident commencing on or about June 7, 2024 in substantially the same form as the letter attached hereto. Carolina Foods is offering the affected resident with complimentary membership with a credit monitoring service. Carolina Foods is advising the affected resident about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected resident are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Carolina Foods, protecting the privacy of personal information is a top priority. Carolina Foods is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Carolina Foods continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

If you have any additional questions, please contact me at (248) 593-2952 or cbattersby@mcdonaldhopkins.com.

Very truly yours,



Colin M. Battersby

Encl.



[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to Carolina Foods, LLC, ("Carolina Foods"). We are writing with important information regarding a security incident that involved some of your personal information. We want to provide you with information about the incident, tell you about the services that we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On March 12, 2024, Carolina Foods detected unauthorized access within our network environment.

What We Are Doing.

Upon learning of this issue, Carolina Foods contained the threat and immediately commenced a prompt and thorough investigation with external cybersecurity professionals experienced in handling these types of incidents. Following the conclusion of an extensive forensic investigation and thorough manual review, Carolina Foods determined on May 8, 2024 that some of your personal information was accessed and acquired in connection with this incident.

What Information Was Involved?

The potentially accessed and acquired information included your full name, social security number, and one or more of the following, to the extent it is in our records: passport and or driver's license.

What You Can Do.

We have no evidence that any of your personal information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. We are offering a complimentary [REDACTED] membership in Identity Defense Complete. For more information on identity theft prevention and the credit monitoring product being offered to you, including instructions on how to activate your complimentary [REDACTED] membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements, explanation of benefits, and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this incident occurred. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against potential misuse of your information. The response line is available Monday through Friday from 9:00am – 9:00pm EST.

Sincerely,

Carolina Foods, LLC

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary [REDACTED] Credit Monitoring.

To enroll in Identity Defense Complete, visit [REDACTED]

1. Enter your unique Activation Code [REDACTED]
Enter your Activation Code and click 'Redeem Code'.
2. Create Your Account
Enter your email address, create your password, and click 'Create Account'.
3. Register
Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Complete Activation
Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is [REDACTED]. After [REDACTED], the enrollment process will close, and your Identity Defense code will no longer be active. If you do not enroll by [REDACTED], you will not be able to take advantage of Identity Defense, so please enroll before the deadline.

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at [REDACTED].

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial one-year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(800) 349-9960
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, 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 reporting company will send you a confirmation letter containing 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.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.