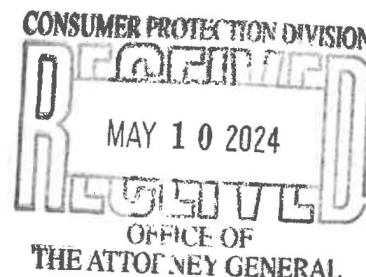


Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

May 3, 2024

VIA U.S. MAIL

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



Re: BRHPAN II – Georgia, LLC – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents BRHPAN II – Georgia, LLC and affiliated entities (“Bluegrass”). I am writing to provide notification of an incident at Bluegrass that may affect the security of personal information of approximately give (5) Maryland residents for whom it had a last known home address. The Bluegrass investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Bluegrass does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Bluegrass recently learned that an unauthorized party may have gained access to a single Bluegrass email account. Upon learning of this issue, Bluegrass immediately commenced a prompt and thorough investigation in consultation with external cybersecurity professionals who regularly investigate and analyze these types of situations. After an extensive investigation and manual document review, Bluegrass discovered on April 3, 2024 that certain files within the email account containing a limited amount of personal information may have been accessed and acquired by the unauthorized party on December 15, 2023, including the affected residents’ full names and Social Security numbers.

To date, Bluegrass 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, Bluegrass wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Bluegrass is providing the affected residents with written notification of this incident commencing on or about May 3, 2024 in substantially the same form as the letter attached hereto. Bluegrass is offering the affected residents whose Social Security numbers were impacted complimentary memberships with a credit monitoring service. Bluegrass is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Baltimore | Chicago | Cleveland | Columbus | Detroit | West Palm Beach
mcdonaldhopkins.com

Page 2

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

Should you have any questions concerning this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

A handwritten signature in blue ink, appearing to read 'D. Paluzzi', is written over the printed name.

Dominic A. Paluzzi

Encl.

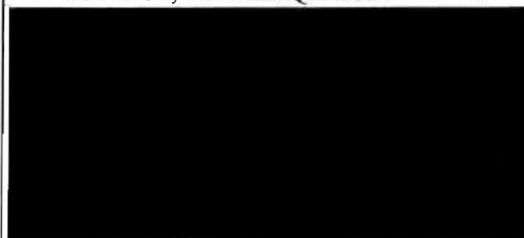


BRHPAN II – Georgia, LLC

P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code: [REDACTED]
To Enroll, Scan the QR Code Below:



Or Visit:

[REDACTED]

May 3, 2024

[REDACTED]

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to BRHPAN II – Georgia, LLC and affiliated entities (collectively, “Bluegrass”). We are writing with important information regarding a recent data security incident. We want to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

We recently learned that an unauthorized party may have gained access to a single Bluegrass email account.

What We Are Doing.

Upon learning of this issue, we immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, we discovered on April 3, 2024 that certain files within the email account containing personal information may have been accessed and acquired by the unauthorized party on December 15, 2023.

What Information Was Involved?

The files that may have been accessed and acquired contained your full name and [REDACTED]

What You Can Do.

To date, we are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. Nevertheless, to protect you from potential misuse of your information, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: [REDACTED] months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

This letter also provides other precautionary measures to protect your personal information, including placing a fraud alert, placing a security freeze, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this incident occurred. We are 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 and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, we encourage you to contact [REDACTED] with any questions and to enroll in the free identity protection services by calling [REDACTED], going to [REDACTED], or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from [REDACTED] Pacific Time. Please note the deadline to enroll is August 3, 2024.

Sincerely,

BRHPAN II – Georgia, LLC

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary [REDACTED]-Month Credit Monitoring.

Website and Enrollment. Scan the QR image or go to [REDACTED] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at [REDACTED] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 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) 685-1111

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. Consider 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 30348-5788

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

(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 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.

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.

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.