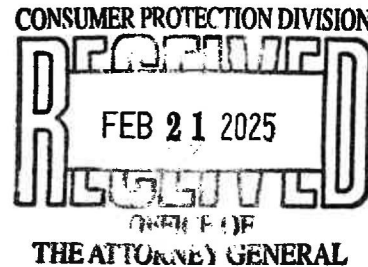


Sean J. Bowen
Direct Dial: 248.402.4067
E-mail: sbowen@mcdonaldhopkins.com

February 11, 2025

VIA U.S. MAIL

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



Re: The Big Green Egg, Inc. – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents The Big Green Egg, Inc. I am writing to provide notification of an incident at The Big Green Egg, Inc. that may affect the security of personal information of one (1) Maryland resident. By providing this notice, The Big Green Egg, Inc. does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On July 29, 2024, The Big Green Egg, Inc. learned that an unauthorized party may have gained limited access to parts of its network. The Big Green Egg, Inc. immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to analyze the extent of any compromise of the information on its network. Based on its comprehensive investigation and manual document review, The Big Green Egg, Inc. discovered on January 9, 2025 that certain files within its network containing personal information may have been accessed and acquired by the unauthorized party in connection with this incident, including the affected resident's payment card access information.

To date, The Big Green Egg, Inc. 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, The Big Green Egg, Inc. 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. The Big Green Egg, Inc. is providing the affected resident with written notification of this incident commencing on or about February 11, 2025 in substantially the same form as the letter attached hereto. The Big Green Egg, Inc. 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 is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Page 2

At The Big Green Egg, Inc., protecting the privacy of personal information is a top priority. The Big Green Egg, Inc. is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. The Big Green Egg, Inc. 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) 402-4067 or sbowen@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

A handwritten signature in black ink, appearing to be 'S. Bowen', with a long horizontal line extending to the right.

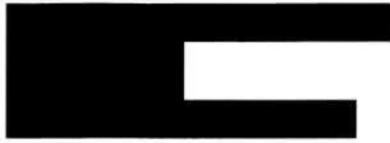
Sean J. Bowen

Encl.

The Big Green Egg, Inc.

P.O. Box 989728

West Sacramento, CA 95798-9728



Enrollment Code: [REDACTED]

To Enroll, Scan the QR Code Below:



Or Visit:



IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to the Big Green Egg, Inc. 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 discovered unauthorized access to certain systems in our network environment.

What We Are Doing.

Upon detecting the incident, we immediately commenced a prompt and thorough investigation, which included containing and securing the email environment, and changing account passwords. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents to investigate the extent of the incident and what, if any, sensitive data, including personal information may have been accessed and/or acquired by the unauthorized party. After an extensive forensic investigation and manual document review, we discovered that certain impacted files containing personal information may have been subject to unauthorized access or acquisition between July 26, 2024 and July 29, 2024. On February 4, 2025 we confirmed your address and moved to promptly notify you.

What Information Was Involved?

The information potentially involved includes 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 providing you with identity theft protection services through IDX, a ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: [REDACTED] 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. To the extent it is helpful, we have also provided information on protecting your medical information on the following pages.

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.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling [REDACTED], by going to [REDACTED], or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from [REDACTED] Eastern Time. Please note the deadline to enroll is [REDACTED].

Sincerely,

The Big Green Egg, Inc.
3786 DeKalb Technology Parkway
Atlanta, GA 30340

– 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. Protecting Your Medical Information.

If this notice letter indicates that your medical information was impacted, we have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

6. 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.

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.

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.