

September 8, 2024

VIA E-MAIL

Attorney General Anthony G. Brown
200 St. Paul Place
Baltimore, MD 21202

E-Mail: idtheft@oag.state.md.us

Re: Notice of Data Breach

Dear Attorney General Brown:

We are writing on behalf of our client, Menu Maker Foods, LLC d/b/a Graves Foods ("Graves Foods"), to inform you of a data incident.

On October 23, 2023, Graves Foods became aware of deployment of ransomware in its legacy computer system. That same day, Graves Foods activated its incident response plan and took steps to contain the incident. Graves Foods also promptly began an investigation with the assistance of third-party cybersecurity experts to determine the nature and scope of the activity, assist with containment, and ensure no ongoing unauthorized activity.

Graves Foods's investigation determined that one user account, one computer, and one legacy Network Attached Storage device (NAS) had been compromised by the attack. The NAS at issue was public facing from a decommissioned service, however the public link remained open. Graves Foods was not able to identify the date that the ransomware was installed. To remediate this vulnerability, the public link was immediately severed, and the computer was taken offline and decommissioned. Graves Foods also rotated all service account passwords (system-to-system accounts) and required all users to change their passwords. Graves Foods has not identified evidence this incident spread beyond Graves Foods to other companies or systems.

Based on Graves Foods's investigation, it appears that the information of one Maryland resident may have been affected, including the individual's name, mailing address, phone number, email address, date of birth, social security number, and/or government issued identification number. Graves Foods has not determined if this individual had their information actually accessed by the threat actor. Nevertheless, notification to the individual will be sent on September 9, 2024 out of an abundance of caution. A sample copy of Graves Foods's notice is attached.



Attorney General Anthony G. Brown
September 8, 2024
Page 2

We assure you that our client, Graves Foods, takes this issue, and the privacy and security of its customers, very seriously. If you have any questions or require further information, please feel free to contact me at wdeagle@sheppardmullin.com or (858) 720-8947.

Sincerely,

A handwritten signature in black ink that reads "Wynter L. Deagle".

Wynter L. Deagle



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Re: Notice of a Data Breach

We are writing to inform you of a ransomware attack against Graves Foods that may affect the privacy of some of your personal information.

What Happened?

On October 23, 2023, Graves Foods became aware of deployment of ransomware in its legacy computer system. That same day, Graves Foods activated its incident response plan and took steps to contain the incident. Graves Foods also promptly began an investigation with the assistance of third-party cybersecurity experts to determine the nature and scope of the activity, assist with containment, and ensure no ongoing unauthorized activity.

Our investigation determined that one user account, one computer, and one legacy Network Attached Storage device (NAS) had been compromised by the attack. The NAS at issue was public facing from a decommissioned service, however the public link remained open. Graves Foods was not able to identify the date that the ransomware was installed. To remediate this vulnerability, the public link was immediately severed, and the computer was taken offline and decommissioned. Graves Foods also rotated all service account passwords (system-to-system accounts) and required all users to change their passwords.

Graves Foods has not identified evidence this incident spread beyond Graves Foods to other companies or systems. This notice has not been delayed by law enforcement.

What Information Was Involved?

The information that may have been accessed included your name, mailing address, phone number, email address, date of birth, social security number, and/or government issued identification number.

What We Are Doing

Graves Foods takes this event very seriously. After becoming aware of the deployment of ransomware, we promptly began an investigation and took action to address the activity. We have been working with outside cybersecurity experts and have implemented specific steps to safeguard against future attacks.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll, a global leader in risk mitigation and response, to provide identity monitoring for <<Monitoring Term Length (Months)>> months at no cost to you. Kroll and its team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

Identity monitoring services available to you include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of the identity monitoring services available to you.

You have until <<b2b_text_6 (activation deadline)>> to activate the identity monitoring services.

Membership Number: <<Membership Number s_n>>

Additional information describing the services is included with this letter. For more information about Kroll and Identity Monitoring services, you can visit its website at: <https://www.info.krollmonitoring.com/>

The enclosed “Steps You Can Take to Protect Your Personal Information”, provides additional information you can use to help protect your information.

For More Information

We understand that you may have questions about this incident that are not addressed in this letter. We have established a dedicated call center available toll free in the U.S. at **(866) 810-9052**, from 8:00 a.m. to 5:30 p.m. Central Time (excluding weekends and major U.S. holidays).

Your privacy is of the utmost importance to us, and we sincerely regret any concern this incident may cause you.

Sincerely,

Graves Foods

Steps You Can Take to Protect Your Information

Monitor Your Accounts.

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Request A Security Freeze on your Credit Report.

You can place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19016
1-888-909-8872

www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348
1-888-298-0045

[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order to request a security freeze, you will need to provide your full name, social security number, date of birth, Social Security number; your residential addresses for the past five years, proof of current address, and a copy of a government-issued identification card

Place A Fraud Alert on Your File.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289

[www.transunion.com/fraud-victim-
resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-836-6351

[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

Additional Information.

You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.identitytheft.gov; 1-877-438-4338; and TTY: 1-866-653-4261. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should be reported to law enforcement and your state Attorney General.

For District of Columbia residents: The District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov. **For Maryland residents,** the Attorney General can be contacted by mail at 200 St. Paul Place, Baltimore, MD, 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at www.marylandattorneygeneral.gov.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. **For New York residents,** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>. **For North Carolina Residents:** The North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400, and online at www.ncdoj.gov. **For Oregon Residents:** You can obtain information from the Oregon Attorney General’s Office about preventing identity theft. You can contact the Oregon Attorney General at: Oregon Department of Justice 1162 Court St. NE Salem, OR 97301 1-(877) 877-9392 (toll-free) <https://www.doj.state.or.us/>. **For Rhode Island Residents:** The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately 367 Rhode Island residents impacted by this incident. This notice has not been delayed by a law enforcement investigation.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you’ll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of identity theft, and then work to resolve it.

Kroll’s activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.