



Blair L. Dawson
550 West Adams Street, Suite 300
Chicago, Illinois 60661
Blair.Dawson@lewisbrisbois.com
Direct: 312.463.3332

January 14, 2022

File No. 30841.1678

VIA U.S. Mail

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Attorney General Brian E. Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Grandizio Wilkins Little & Matthews, LLP (“GWLM”) in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland’s breach notification statute.

1. Nature of the Security Incident

GWLM is an accounting firm based out of Sparks, Maryland.

On June 7, 2021, GWLM discovered unauthorized access to an employee’s email account. Upon discovering this activity, GWLM took steps to secure our email system and launched an investigation into the matter. We immediately engaged cybersecurity experts to determine if information had been affected. On December 17, 2021 the investigation determined personal information may have been impacted as a result of the incident. GWLM then worked diligently to determine the individuals who were impacted and their address information in order to provide notification of this incident. On January 14, 2022 GWLM is sending notice to impacted individuals by U.S. Mail.

2. Type of Information and Number of Maryland Residents Involved

The incident involved personal information for approximately 9,041 Maryland residents. The files that may have been accessed by the unauthorized individual may have contained your name, Social Security Number, Medical Information, Driver's License Information, Financial Account Information, or Payment Card Information.

GWLM notified the impacted Maryland residents of this data security incident via first class U.S. mail on January 14, 2022, providing 12 months of credit monitoring.

Measures Taken to Address the Incident

In response to the incident, GWLM retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. Additionally, GWLM reported the incident to the Federal Bureau of Investigation ("FBI") and will cooperate fully and assist with any investigation. GWLM Advisors also implemented additional security measures to further harden our digital environment in an effort to prevent a similar event from occurring in the future and revised their data retention policy.

Finally, GWLM is notifying the affected individuals and providing them with steps they can take to protect their personal information, including enrolling in the complimentary identity monitoring services offered in the notification letter.

3. Contact Information

GWLM is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact Blair Dawson at 312-463-3332 or Blair.Dawson@lewisbrisbois.com.

Sincerely,
/s/ Blair Dawson
Blair L. Dawson of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

BLD:sgg

Encl.: Sample Consumer Notification Letters



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

To Enroll, Please Call:
1-833-648-2047
Or Visit:
<https://response.idx.us/gwlm>
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

January 14, 2022

Re: <<Variable Text 1>>

Dear <<FIRST NAME>> <<LAST NAME>>,

I am writing to inform you of a data security incident experienced by Grandizio Wilkins Little & Matthews, LLP ("GWLM") that involved your personal information. We take the privacy and security of your personal information very seriously. This letter contains information about the incident and steps you can take to ensure your personal information is protected.

What Happened? On June 7, 2021, we discovered unauthorized access to a GWLM employee's email account. Upon discovering this activity, we took steps to secure our email system and launched an investigation into the matter. We immediately engaged cybersecurity experts to determine if information had been affected. On December 17, 2021 at completion of our investigation, we learned that your information may have been involved in a data security incident. While at this time we still have no evidence that any information was accessed or misused, out of an abundance of caution we are providing identity theft protection to those whose information may have been in the affected systems.
<<Variable Text 2>>

What Information Was Involved? The files that may have been accessed by the unauthorized individual may have contained your name, Social Security Number, Medical Information, Drivers License Information, Financial Account Information, or Payment Card Information.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We have secured the services of IDX to provide credit and identity monitoring at no cost to you for <<12 / 24>> months. IDX is a global leader in risk mitigation and response, and its team has extensive experience helping people who have sustained an unintentional exposure of confidential data. The IDX services include credit monitoring; identity monitoring; \$1 million in identity theft expense reimbursement insurance; and fraud prevention and resolution support.

To receive credit services, you must be over the age of 18, 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.

Please note you must enroll by **April 14, 2022**. If you have questions or need assistance, please call IDX at 1-833-648-2047.

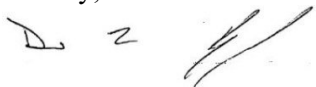
What You Can Do: Please review the enclosed "Additional Resources" page. It describes additional steps you can take to help safeguard your information, including recommendations by the Federal Trade Commission regarding identity

theft protection and details on how to place a fraud alert or a security freeze on your credit file. We also encourage you to activate the complimentary identity monitoring services we are making available through IDX.

For More Information: If you have questions or need assistance, please call 1-833-648-2047, Monday through Friday from 9 a.m. to 9 p.m. Eastern Time. Please have your enrollment code ready.

Protecting your information is important to us. Please know that we take this incident very seriously and deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in dark ink, appearing to read "D. L. Harrington, JR.", with a stylized flourish at the end.

Daniel L. Harrington, JR.
Managing Partner
Grandizio, Wilkins, Little & Matthews, LLP

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion	Experian	Equifax	Free Annual Report
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-800-909-8872	1-888-397-3742	1-800-685-1111	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Contact information for the FTC is: **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov and www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

New York Attorney General	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
Bureau of Internet and Technology Resources	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
28 Liberty Street	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
New York, NY 10005	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
ifraud@ag.ny.gov	1-888-743-0023	1-877-566-7226	401-274-4400
1-212-416-8433			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf

