



Maria Efaplatidis
77 Water Street, Suite 2100
New York, NY 10005
Maria.Efaplatidis@lewisbrisbois.com
Direct: 212.232.1366

January 3, 2022

VIA E-MAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Fax: (410) 576-6566
Email: Idtheft@oag.state.md.us

Re: Data Security Incident Notice

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Walton Isaacson 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 data breach statute.

1. Nature of the Security Incident

Walton Isaacson is a marketing firm based in Los Angeles, California.

On November 17, 2021, Walton Isaacson discovered unusual activity affecting Walton Isaacson's computers. Walton Isaacson information technology personnel immediately launched an investigation to determine what happened. Walton Isaacson also engaged cybersecurity experts to assist with the investigation. The investigation determined that Walton Isaacson had experienced a malware incident and that an unknown actor may have gained access to and obtained data from the Walton Isaacson network without authorization. Walton Isaacson then worked to identify and review the information that was involved. On December 11, 2021, it was determined that some personal information may have been included in the information involved in the incident.

2. Type of Information and Number of Maryland Residents Involved

The incident involved personal information for 2 Maryland residents. The information involved the individuals' name and a Social Security Number.

The affected individuals will receive a letter notifying them of the incident and providing additional steps they can take to protect their personal information. For individuals whose Social Security numbers were potentially impacted, Walton Isaacson will be offering complimentary identity monitoring services. The notification letters will be sent via USPS First Class Mail on January 3, 2022. A sample copy of the notification letter sent to the affected individuals is attached.

3. Measures Taken to Address the Incident

In response to the incident, Walton Isaacson retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. Walton Isaacson is cooperating with the Federal Bureau of Investigation and will provide whatever assistance is necessary to attempt to hold the perpetrators of this incident accountable, if possible.

Additionally, as discussed above, Walton Isaacson is notifying the affected individuals and providing them with steps they can take to protect their personal information.

4. Contact Information

Walton Isaacson 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 Maria Efaplatidis at Maria.Efaplatidis@lewisbrisbois.com.

Sincerely,

Maria Efaplatidis of
LEWIS BRISBOIS BISGAARD & SMITH LLP

cc: Walton Isaacson

Encl: Sample Individual Notification Letter



Walton Isaacson

10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

January 3, 2022

Re: Notice of Data Security incident

Dear <<First Name>> <<Last Name>>,

Walton Isaacson is writing to notify you of a recent data security incident that may have involved your personal information. Walton Isaacson takes the privacy and security of your personal information very seriously. We want to inform you of this incident and about steps you can take to help protect your personal information and offer you complimentary credit monitoring and identity protection services.

What Happened? On or about November 17, 2021, Walton Isaacson became aware of unusual activity affecting Walton Isaacson's computers. Walton Isaacson information technology personnel immediately launched an investigation to determine what happened. We also engaged cybersecurity experts to assist with the investigation. The investigation determined that we had experienced a malware incident and that an unknown actor may have gained access to and obtained data from the Walton Isaacson network without authorization. We then worked to identify and review the information that was involved. On December 11, 2021, we determined that some of your personal information may have been included in the information involved in the incident. This is why we are informing you of the incident and providing you with access to complementary identity monitoring protection services from IDX. We have no information at this time that your information has been misused.

What Information Was Involved? The following information may have been impacted in connection with this incident: your name and Social Security Number.

What We Are Doing. After discovering the incident, Walton Isaacson implemented additional security features to reduce the risk of a similar incident occurring in the future. We are cooperating with the Federal Bureau of Investigation and will provide whatever assistance is necessary to attempt to hold the perpetrators of this incident accountable, if possible.

We are further notifying you of this event and advising you about steps you can take to help protect your information. In addition, out of an abundance of caution, we are offering you complimentary credit monitoring and identity protection services for twelve months at no cost to you through IDX. IDX is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include 24 months of Single Bureau Credit Monitoring.

Additional information describing your services is included with this letter.

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.

Visit <https://app.idx.us/account-creation/protect> to activate and take advantage of your identity monitoring services.

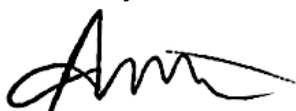
*You have until **April 3, 2022**, to activate your identity monitoring services.*

Enrollment Code: **Found above.**

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call our dedicated call center at 1-800-939-4170 from 6:00 a.m. to 6:00 p.m. Pacific Time, Monday through Friday. IDX representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'A. Walton', with a stylized flourish at the end.

Aaron Walton
CEO
Walton Isaacson

Steps You Can Take to Protect Your Personal 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 24 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 www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.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 one year. 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: 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.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

California Attorney General's Office

P.O. Box 944255
Sacramento, CA 94244
<https://oag.ca.gov/>
1-800-952-5225

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 other rights. 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.