



Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

January 24, 2022

Via Electronic Mail

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

Re: **Notification of Data Security Incident**

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Walsworth Publishing Company ("Walsworth"), a printing and binding company located in Marceline, Missouri, in connection with a recent data security incident described in greater detail below.

1. Nature of the Security Incident

On October 21, 2021, Walsworth discovered unusual activity relating to one Walsworth employee email account. Walsworth immediately took steps to investigate the activity and to provide additional security to its email environment. Walsworth conducted an investigation into what happened and whether any personal information may have been impacted. Through the investigation, Walsworth learned that one email account was accessed without authorization by an unknown individual. Walsworth reviewed the contents of the impacted email account and on December 1, 2021, confirmed that some sensitive, personal information was contained within the email account. Thereafter, Walsworth worked to identify address information for the impacted individuals and prepared notification materials.

2. Type of Information and Number of Maryland Residents Involved

A total of 7 residents of Maryland were notified about this incident. The information involved may include name, Social Security number, health care information, bank account information, username and password information, and personal email address.

Affected individuals will receive a letter notifying them of the incident, offering complimentary identity protection services, and providing additional steps they can take to protect their personal information. The notification letters will be sent via USPS First Class Mail on January 20, 2022.

3. Measures Taken to Address the Incident

Upon learning of this incident, Walsworth took steps to secure the impacted email platform and further secured its environment. Additionally, Walsworth engaged a computer forensics firm to conduct an investigation into the incident. Finally, Walsworth has notified the potentially impacted individuals and provided them with information about steps they can take to help protect their personal information as well as offering complimentary identity protection services, 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

4. Contact Information

Walsworth 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 Lindsay Nickle at Lindsay.Nickle@lewisbrisbois.com.

Sincerely,



Lindsay Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Walsworth Publishing Company
10300 SW Greenburg Rd., Suite 570
Portland, OR 97223

Walsworth®

To Enroll, Please Call:
1-833-676-2184

Or Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code: [XXXXXXXXXX]

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

January 20, 2022

Re: Notice of Data Security Incident

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

I am writing to inform you about a recent incident experienced by Walsworth Publishing Company (“Walsworth”) that may have impacted your personal information. Please read this letter carefully as it contains information regarding the incident and information about steps that you can take to help protect your personal information.

What Happened: On October 21, 2021, Walsworth discovered unusual activity relating to one Walsworth employee email account. Walsworth immediately took steps to investigate the activity and to provide additional security to its email environment. Walsworth conducted an investigation into what happened and whether any personal information may have been impacted. Through the investigation, Walsworth learned that one email account was accessed without authorization by an unknown individual. Walsworth reviewed the contents of the impacted email account, and, on December 1, 2021, Walsworth learned that some of your personal information was contained within the email account. Walsworth has been working diligently to provide you with notification of this incident. Please note that we are not aware of the misuse of any personal information.

What Information Was Involved: The information that may have been involved included your name, <<variable text>>.

What We Are Doing: As soon as Walsworth learned of this incident, Walsworth took the steps described above. In addition, Walsworth implemented additional measures to enhance the security of its email environment in an effort to minimize the likelihood of a similar event occurring in the future.

Walsworth is also providing you with information regarding steps that you can take to help protect your information. As an added precaution, Walsworth is offering you complimentary identity protection services through IDX, a data breach and recovery services expert. Your services include <<12 or 24>> 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. Please note the deadline for you to enroll in the services being offered to you is April 20, 2022.

What You Can Do: Although Walsworth is not aware of the misuse of any information potentially impacted in connection with this incident, Walsworth encourages you to review the recommendations on the following page to help protect your information. Walsworth also encourages you to contact IDX with any questions and to enroll in the free identity protection services being offered to you by calling 1-833-676-2184 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday

from 6am – 6pm Pacific Time. IDX representatives are fully versed on the incident and can answer questions or concerns you may have regarding protection of your information.

For More Information: If you have any questions regarding this incident or would like assistance enrolling in the services offered, please call 1-833-676-2184, Monday through Friday from 6am – 6pm Pacific Time. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

The security of employee information is a top priority for Walsworth, and Walsworth is committed to safeguarding your data. We sincerely apologize for any inconvenience that this matter may cause.

Sincerely,

A handwritten signature in black ink that reads "Bob Perkins". The signature is written in a cursive, flowing style.

Bob Perkins
Executive Vice President of Human Resources
Walsworth Publishing Company

Additional Steps You Can Take to 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).

Request a Copy of Your 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 <https://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 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

Place a 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 <https://www.annualcreditreport.com>.

Put a 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 (FTC)

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

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

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

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

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 <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.