Maria Efaplomatidis
175 Pearl Street
Suite C-402
Brooklyn, New York 11201
mefaplomatidis@constangy.com
917.414.8991

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

November 22, 2024

VIA ONLINE SUBMISSION

Attorney General Bob Ferguson
Office of the Attorney General
Consumer Protection Division
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100
Tel: 206-464-6684

Re: Notice of Data Event

To Whom It May Concern:

We represent Walsworth Publishing Company ("Walsworth") located at 306 N. Kansas Ave, Marceline, Missouri 64658 and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately 685 Washington residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Walsworth does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

1. Nature of the Data Event

On February 9, 2024, Walsworth was alerted to the occurrence of a potential data security incident involving its website and purchasing page. Walsworth promptly took steps to secure the website and hired cybersecurity specialists to conduct an investigation to determine the nature and scope of the issue. Although the investigation did not find evidence of personal data exposure, Walsworth chose to notify customers out of an abundance of caution. After an in-depth review of the potential data involved, Walsworth determined on November 1, 2024, that sensitive customer information was potentially involved.

The information that could have been subject to unauthorized access includes first and last name, as well as payment card number, expiration date, and CVV or security code.

2. Notice to Washington Residents

On or about November 22, 2024 Walsworth provided written notice of this incident to approximately 685 Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

3. Other Steps Taken and To Be Taken

Upon discovering the event, Walsworth moved quickly to investigate and respond to the incident, assess the security of Walsworth systems, and identify potentially affected individuals. Walsworth is also working to implement additional safeguards and training to its employees. Walsworth is providing access to credit monitoring services for 12 months, through CyEx, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Walsworth is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Walsworth is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Walsworth is providing written notice of this incident to relevant state and industry regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

4. Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 917.414.8991.

Sincerely,

Maria Efaplomatidis
Partner

Exhibit A

Walsworth®

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Re: Notice of Data <<Variable Text 1>>

Dear <<Full Name>>:

I am writing to inform you that Walsworth Publishing Company ("Walsworth") recently experienced a data security incident which may have impacted your personal information. Walsworth takes the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and information about steps that you can take to help protect your information, including enrolling in the complimentary credit monitoring and identity protection services we are making available to you.

What Happened? On February 9, 2024, Walsworth was alerted to the occurrence of a potential data security incident involving its website and purchasing page. Walsworth promptly took steps to secure the website and hired cybersecurity experts to conduct an investigation to determine the nature and scope of the issue. Although the investigation did not find evidence of personal data exposure, Walsworth chose to notify customers out of an abundance of caution. After an in depth review of the potential data involved, Walsworth determined on November 1, 2024, that your customer information was potentially involved.

What Information was Involved? The information that may have been affected in connection with this incident includes your name as well as your payment card number, expiration date, and CVV or security code.

What Are We Doing? As soon as Walsworth discovered the potential incident, Walsworth took the steps discussed above. In addition, Walsworth coordinated efforts with the payment card processor and will work with them in any investigation. In order to reduce the likelihood of a similar incident occurring in the future, Walsworth also implemented additional measures to enhance the security of its website.

In addition, Walsworth is providing you with access to <<12/24>> months of complimentary identity protection services through CyEx, a global technology services leader. The deadline to enroll in these services is <<Enrollment Deadline>>.

What You Can Do. You can follow the recommendations included with this letter to protect your personal information. Walsworth recommends that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

In addition, you can contact CyEx representatives who will work on your behalf to help resolve issues you may experience as a result of this incident.

To Enroll: To enroll in CyEx Identity Defense visit https://app.identitydefense.com/enrollment/activate/wal

1. Enter your unique Activation Code <<Activation Code>>
   Enter your Activation Code and click 'Redeem Code'.
2. Create Your Account
   Enter your email address, create your password, and click 'Create Account'.
3. Register
   Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Complete Activation
   Click 'Continue to Dashboard' to finish enrolling.

Please note the deadline to enroll in these complimentary services is <<Enrollment Deadline>>. Please do not discard this letter, as you will need the Activation code provided above to access services.

For More Information: If you have questions about this letter or need assistance, please do not hesitate to reach out to our designated call center at 1-888-596-4730, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding holidays and they will be happy to provide you with additional information.

We take your trust in Walsworth and this matter very seriously. Please accept our apologies for any concern or inconvenience this may cause you.

Sincerely,

Mike Sargent
Vice President of Technology
Walsworth Publishing Company
306 N Kansas Ave
Marceline, MO 64658

STEPS YOU CAN TAKE TO HELP 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 2000
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
There are <<RI#>> RI residents impacted.

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.

Walsworth®

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Re: Notice of Data <<Variable Text 1>>

Dear <<Full Name>>:

I am writing to inform you that Walsworth Publishing Company ("Walsworth") recently experienced a data security incident which may have impacted your personal information. Walsworth takes the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and information about steps that you can take to help protect your information, including enrolling in the complimentary credit monitoring and identity protection services we are making available to you.

What Happened? On February 9, 2024, Walsworth was alerted to the occurrence of a potential data security incident involving its website and purchasing page. Walsworth promptly took steps to secure the website and hired cybersecurity experts to conduct an investigation to determine the nature and scope of the issue. Although the investigation did not find evidence of personal data exposure, Walsworth chose to notify customers out of an abundance of caution. After an in depth review of the potential data involved, Walsworth determined on November 1, 2024, that your customer information was potentially involved.

What Information was Involved? The information that may have been affected in connection with this incident includes your name as well as your payment card number, expiration date, and CVV or security code.

What Are We Doing? As soon as Walsworth discovered the potential incident, Walsworth took the steps discussed above. In addition, Walsworth coordinated efforts with the payment card processor and will work with them in any investigation. In order to reduce the likelihood of a similar incident occurring in the future, Walsworth also implemented additional measures to enhance the security of its website.

In addition, Walsworth is providing you with access to <<12/24>> months of complimentary identity protection services through CyEx, a global technology services leader. The deadline to enroll in these services is <<Enrollment Deadline>>.

What You Can Do. You can follow the recommendations included with this letter to protect your personal information. Walsworth recommends that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

In addition, you can contact CyEx representatives who will work on your behalf to help resolve issues you may experience as a result of this incident.

To Enroll: To enroll in CyEx Identity Defense visit https://app.identitydefense.com/enrollment/activate/wal

1. Enter your unique Activation Code <<Activation Code>>
   Enter your Activation Code and click 'Redeem Code'.
2. Create Your Account
   Enter your email address, create your password, and click 'Create Account'.
3. Register
   Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Complete Activation
   Click 'Continue to Dashboard' to finish enrolling.

Please note the deadline to enroll in these complimentary services is <<Enrollment Deadline>>. Please do not discard this letter, as you will need the Activation code provided above to access services.

For More Information: If you have questions about this letter or need assistance, please do not hesitate to reach out to our designated call center at 1-888-596-4730, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding holidays and they will be happy to provide you with additional information.

We take your trust in Walsworth and this matter very seriously. Please accept our apologies for any concern or inconvenience this may cause you.

Sincerely,

Mike Sargent
Vice President of Technology
Walsworth Publishing Company
306 N Kansas Ave
Marceline, MO 64658

STEPS YOU CAN TAKE TO HELP 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 2000
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
There are <<RI#>> RI residents impacted.

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.