



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Josh Brian
Office: (267) 930-2405
Fax: (267) 930-4771
Email: JBrian@mullen.law

3001 N. Rocky Point Drive East, Suite 200
Tampa, FL 33607

May 11, 2026

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Bloomsbury Publishing, Inc. (“Bloomsbury”) located at 1359 Broadway, 12th Floor, New York, NY 10018, and write to notify your office of a matter that involves personal information relating to approximately four (4) New Hampshire residents. This notice may be supplemented if any new, significant facts are learned subsequent to its submission. By providing this notice, Bloomsbury does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On April 2, 2026, an unknown individual impersonated a Bloomsbury company executive to obtain copies of employees’ 2025 Form W-2s, which included the employees’ names and Social Security numbers. Bloomsbury became aware that this occurred on April 15, and notified the employees by email within 24 hours, and followed up by sending employees notices via written letter.

Notice to New Hampshire Residents

On May 11, 2026, Bloomsbury provided written notice to approximately four (4) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon learning of this matter, Bloomsbury moved quickly to understand what happened, implement additional controls to reduce the risk of a matter like this reoccurring, and notify its employees. Further, Bloomsbury notified federal law enforcement regarding the event. As part of its additional controls, Bloomsbury is working to implement additional safeguards and training to its employees, and to increase the aggressiveness of its email spam filtering. Bloomsbury is providing access to credit monitoring services for two (2) years, through IDX, to notified individuals, at no cost to these individuals.

Additionally, Bloomsbury is providing notified individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of tax return fraud to the Internal Revenue Service and state tax authority. Bloomsbury is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

Contact Information

Should you have any questions regarding this notification or other aspects of this matter, please contact us at (267) 930-2405.

Very truly yours,



Josh Brian of
MULLEN COUGHLIN LLC

JPB/ahf
Enclosure

EXHIBIT A

Bloomsbury Publishing, Inc.
Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<PostalCode+4>>

Enrollment Code: <<XXXXXXXXXX>>

Enrollment Deadline: August 11, 2026

To Enroll, Scan the QR Code Below:



Or Visit:

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

May 11, 2026

<<Notice of Data Breach (CA Only)>>

Dear <<FirstName>> <<LastName>>:

We write to inform you about a matter that involves your 2025 W-2 tax form. This letter provides you with information about this matter, our response, and steps you may take to protect your information in response to this matter.

What Happened? On April 2, 2026, an unknown individual impersonated a company executive to obtain copies of employees' 2025 Form W-2s, which included your Form W-2. We became aware that this happened on April 15, 2026.

What Information Was Involved? Your Form W-2 was involved with this matter, which contained your name and Social Security number.

What We Are Doing. We are increasing our social engineering and phishing training frequency to reinforce our protocols and guidance for handling personal information. Additionally, we are strengthening our email filters to help reduce the risk of an issue like this reoccurring. We also notified the Federal Bureau of Investigation and will assist with their investigation of this matter. In addition to these steps, we are also providing you with two (2) years of complimentary identity monitoring through IDX.

What Individuals Can Do. We encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing their account statements and monitoring their free credit reports for suspicious activity and to detect errors. We also encourage individuals to review the "Steps Individuals Can Take To Protect Personal Information" section of this letter. This section contains free resources that are available, including guidance for monitoring free credit reports, how to place a fraud alert or security freeze on credit files, and contact information for the consumer reporting agencies and Federal Trade Commission. Individuals may also enroll in the identity monitoring, which is being provided for free. The enrollment instructions are in the "Enroll in Monitoring Services" section of this correspondence. The credit monitoring is being provided to you at no cost. Please note that, due to privacy restrictions, we are unable to automatically enroll individuals in the complimentary credit monitoring.

In addition to the above steps that you can take, you are encouraged to file your 2025 tax return as soon as possible, if you have not already done so. You can visit the Internal Revenue Service's ("IRS") website at <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft> for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. If you are aware or become aware of a fraudulent tax return filed in your name or you are instructed to do so by the IRS, you should file the IRS Form 14039, Identity Theft Affidavit, with a paper copy of the return, and mail according to the

instructions. A copy of this form can be found at <https://www.irs.gov/pub/irs-pdf/f14039.pdf> or <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft>. You should also look at the information made available by the tax authority for your state of residence and any other state where you file a tax return. For a list of websites for each US state's tax authority, visit <https://www.taxadmin.org/state-tax-agencies>.

For More Information. If you have questions about this matter, we have an assistance line with agents ready to help answer your questions. Please contact our toll-free assistance line at 1-833-788-9712, Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time (excluding U.S. holidays). You may also write to us at Bloomsbury Publishing, Inc., Attn: Legal, 1359 Broadway, 12th Floor, New York, NY 10018.

Sincerely,

Bloomsbury Publishing, Inc.

STEPS INDIVIDUALS CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

In response to this matter, we are providing you with access to Single Bureau Credit Monitoring services through IDX at no charge. These services provide you with 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.

1. Website and Enrollment. Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is August 11, 2026.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-788-9712 to gain additional information about this incident and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of IDX's ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Ave NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. 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 also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-442-9828; and oag.dc.gov. You may also contact us at Bloomsbury Publishing, Attn: Compliance, 1359 Broadway, 12th Floor, New York, NY 10018, or 1-212-419-5300.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://oag.maryland.gov>. You may also contact us at Bloomsbury Publishing, Attn: Compliance, 1359 Broadway, 12th Floor, New York, NY 10018, or 1-212-419-5300.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.