



MULLEN  
COUGHLIN<sup>LLC</sup>  
ATTORNEYS AT LAW

Jillian Seifrit  
Office: (267) 930-4651  
Fax: (267) 930-4771  
Email: JSeifrit@mullen.law

426 W. Lancaster Avenue, Suite 200  
Devon, PA 19333

July 31, 2024

**VIA E-MAIL**

Office of the Attorney General  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202  
E-mail: [idtheft@oag.state.md.us](mailto:idtheft@oag.state.md.us)

**Re: Notice of Data Event**

To Whom It May Concern:

We represent National Publisher Services LLC d.b.a. NPS Media Group (“NPS”) located at 52 Golf Oval, Springfield, New Jersey 07081, and are writing to notify your office of an event that may affect the security of certain information relating to one (1) Maryland resident. This notice may be supplemented if new significant facts are learned subsequent to its submission. By providing this notice, NPS does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

On or about May 23, 2024, NPS became aware of suspicious activity on its systems. NPS promptly took steps to secure its systems and launched an investigation to determine the full nature and scope of the event. The investigation determined that an unknown actor gained access to certain NPS systems between April 11, 2024, and April 30, 2024 and likely accessed and/or acquired information on those systems.

NPS then undertook a review of the involved information to determine what was contained therein and to whom it related. The review was completed on or about June 27, 2024. The information that could have been subject to unauthorized access includes name and Social Security number.

### **Notice to Maryland Resident**

On or about July 31, 2024, NPS provided written notice of this event to one (1) Maryland resident. 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 becoming aware of the event, NPS moved quickly to investigate, respond, assess the security of its systems, and identify potentially affected individuals. Further, NPS notified federal law enforcement regarding the event. NPS is also working to implement additional safeguards and training to its employees. NPS is providing access to credit monitoring services for twelve (12) months, through Epiq, to individuals whose information was potentially affected by this event, at no cost to these individuals.

Additionally, NPS is providing impacted individuals with guidance on how to better protect against identity theft and fraud. NPS 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.

NPS is providing written notice of this event to relevant state regulators, as necessary.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4651.

Very truly yours,

Jillian Seifrit of  
MULLEN COUGHLIN LLC

JJS/ahf  
Enclosure

# **EXHIBIT A**



<<Return Mail Address>>

<<Name 1>> <<Name 2>>

<<Address 1>>

<<Address 2>>

<<Date>>

<<City>>, <<State>> <<Zip>>

Dear <<Name 1>> <<Name 2>>:

National Publisher Services LLC d.b.a. NPS Media Group (“NPS”) is writing to inform you of an event that may have impacted some of your information. We are providing you with information about the event, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

**What Happened?** On May 23, 2024, NPS became aware of suspicious activity on our systems. We promptly took steps to secure our systems and launched an investigation to determine the full nature and scope of the event. Our investigation determined that an unknown actor gained access to certain NPS systems between April 11, 2024, and April 30, 2024 and likely accessed and/or acquired information on those systems.

We then undertook a review of the involved information to determine what was contained therein and to whom it related. Our review was completed on or about June 27, 2024.

**What Information Was Involved?** Our investigation determined that your name and Social Security number were contained within the impacted files. To date, there is no indication of identity theft or fraud in relation to this event.

**What We Are Doing.** The privacy and security of information in our possession is one of our highest priorities. Upon learning of this event, we immediately took steps to ensure the security of our systems and investigate the event. Additionally, we are notifying state regulators as required. As part of our ongoing commitment to the privacy of information in our care, we have implemented and continue to implement technical security measures to strengthen the security of our systems. As an additional precaution, we are offering you access to 12 months of complimentary credit monitoring and identity restoration services through Equifax.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Personal Information*. There you will also find more information on the credit monitoring and identity restoration services we are making available to you. NPS will cover the cost of these services; however, you will need to complete the enrollment process. Enrollment instructions are enclosed with this letter.

**For More Information.** If you have additional questions, please contact us at 732-548-8083. You may also write to NPS at 52 Golf Oval, Springfield, New Jersey 07081. Protecting your information is important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

David Goodman  
Partner

## STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

### Enroll in Monitoring Services



Enter your Activation Code: **<ACTIVATION CODE>**

**Enrollment Deadline:** October 31, 2024

### Equifax Credit Watch™ Gold

\*Note: You must be over age 18 with a credit file to take advantage of the product

### Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications<sup>1</sup> when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts<sup>2</sup>, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock<sup>3</sup>
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft<sup>4</sup>

### Enrollment Instructions

Go to [www.equifax.com/activate](http://www.equifax.com/activate)

Enter your unique Activation Code of **<ACTIVATION CODE>** then click “Submit” and follow these 4 steps:

1. **Register:**  
Complete the form with your contact information and click “Continue”.  
*If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.*  
*Once you have successfully signed in, you will skip to the Checkout Page in Step 4*
2. **Create Account:**  
Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**  
To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**  
Upon successful verification of your identity, you will see the Checkout Page.  
Click ‘Sign Me Up’ to finish enrolling.  
**You’re done!**  
The confirmation page shows your completed enrollment.  
Click “View My Product” to access the product features.

---

<sup>1</sup> WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. <sup>2</sup>The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. <sup>3</sup>Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit [www.optoutprescreen.com](http://www.optoutprescreen.com) <sup>4</sup>The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.\

## **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](http://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:

| <b>Equifax</b>                                                                                                                  | <b>Experian</b>                                                             | <b>TransUnion</b>                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a> | <a href="https://www.experian.com/help/">https://www.experian.com/help/</a> | <a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a> |
| 1-888-298-0045                                                                                                                  | 1-888-397-3742                                                              | 1-800-916-8800                                                                              |
| Equifax Fraud Alert, P.O. Box 105069<br>Atlanta, GA 30348-5069                                                                  | Experian Fraud Alert, P.O. Box<br>9554, Allen, TX 75013                     | TransUnion Fraud Alert, P.O. Box<br>2000, Chester, PA 19016                                 |
| Equifax Credit Freeze, P.O. Box 105788<br>Atlanta, GA 30348-5788                                                                | Experian Credit Freeze, P.O.<br>Box 9554, Allen, TX 75013                   | TransUnion Credit Freeze, P.O.<br>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 Avenue NW, Washington, D.C. 20580; [www.identitytheft.gov](http://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 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://www.marylandattorneygeneral.gov/>.

*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>.