



2049 Century Park East Suite 2900, Los Angeles, CA 90067 • 310.556.1801

November 23, 2022

Pasha Sternberg
310.229.1335
psternberg@polsinelli.com

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Office of the Attorney General

Attn: Jeff Karberg, Administrator of the Identity Theft Program

Attn: Security Breach Notification

200 St. Paul Place

Baltimore, Maryland 21202

Re: Notification of a Potential Data Security Incident

Dear Mr. Karberg:

We represent Primmer, Piper, Eggleston, & Cramer (“Primmer”) in connection with an incident that may have involved the personal information of one (1) Maryland resident. Primmer is reporting the incident pursuant to MD. CODE ANN., COM. LAW § 14-3504(H). This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to this submission. While Primmer is notifying you of this incident, Primmer does not waive any rights or defenses relating to the incident or this notice.

NATURE OF THE INCIDENT

In November 2021, Primmer discovered that an unauthorized third party gained access to its network and copied a limited amount of data to a foreign private hosting site. Upon learning of the incident, Primmer immediately took steps to secure its network. Primmer launched an investigation and engaged an IT security firm to assist in its investigation. Primmer also determined the foreign location of the hosting site and worked with the site and law enforcement to lock access to the data within two hours of it being uploaded. It subsequently had the site destroy the copy it was hosting.

While Primmer is not aware of any access to the data on the hosting site, because it could not rule this out as a possibility and out of an abundance of caution, Primmer reviewed the contents of the copied data. On April 14, 2022, Primmer determined that the data contained personal information. For the Maryland resident, the information involved may have included name, Social Security number, and date of birth.

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Nashville New York Phoenix
St. Louis San Francisco Seattle Washington, D.C. Wilmington

Polsinelli PC, Polsinelli LLP in California



November 23, 2022

Page 2

NUMBER OF RESIDENTS NOTIFIED

Primmer recently determined that the incident involved one (1) Maryland resident. Primmer notified involved individuals via written notification between July 25, 2022, and November 15, 2022. Enclosed is a sample of the notice sent to the Maryland resident via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, Primmer worked with a forensic firm to assist in its investigation and confirm the security of its computer systems. For individuals whose Social Security number or driver's license number was potentially involved, Primmer has provided identity protection and credit monitoring services through Experian. In the notification letters, Primmer also provided additional steps individuals can take to protect themselves against fraudulent activity and identity theft. Finally, Primmer continues to implement appropriate safeguards to protect personal information.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

A handwritten signature in dark ink, appearing to read 'Pasha Sternberg'.

Pasha Sternberg

Enclosure



PRIMMER PIPER
EGGLESTON &
CRAMER PC

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Primmer, Piper, Eggleston & Cramer PC values and respects the privacy and confidentiality of your information. Unfortunately, we are writing to advise you of a recent incident that may have involved some of your personal information. **We are not aware of any instances of fraud or identity theft that have occurred as a result of this incident.** This letter provides some additional information about the incident and steps you can take to protect yourself from the misuse of your information.

What Happened? In November 2021, we discovered that an unauthorized third party gained access to our network and copied a limited amount of data to a foreign private hosting site. Immediately upon learning of the incident, we engaged our IT security firm to investigate and confirm the security of our computer systems. We also determined the foreign location of the hosting site and worked with the site and law enforcement to lock access to the data within two hours of it being uploaded, and had the site destroy the hosted data. While we are not aware of any access to the data, out of an abundance of caution, we reviewed the contents of the copied data, and on April 14, 2022, we determined that the data contained your personal information.

What Information Was Involved? The information involved varies by individual, but may have included your <<b2b_text_2 ("name" and data elements)>>.

What We Are Doing. We conducted an investigation into how the incident occurred and are taking steps to reduce the risk of this type of incident occurring in the future. Additionally, although we are not aware of any instances of fraud or identity theft, we are offering a complimentary one-year membership of Experian IdentityWorks Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

What You Can Do. You can find more information on steps to protect yourself against identity theft or fraud, including the tips provided by the FTC on fraud alerts, security and credit freezes, and steps you can take to avoid identity theft in the enclosed *Additional Important Information* sheet. We also encourage you to activate the credit monitoring services provided in this letter.

For More Information. We take our responsibility to safeguard your personal information seriously and we apologize for any inconvenience this incident may cause you. For further information and assistance, please call [number] from 9:00 a.m. – 6:30 p.m. Eastern, Monday through Friday, excluding major US holidays.

Sincerely,

Gary L. Franklin

Managing Shareholder & Board Chair
Primmer, Piper, Eggleston & Cramer PC

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<b2b_text_6 (date)>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: <<Activation Code s_n>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number <<b2b_text_1 (engagement #)>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL IMPORTANT INFORMATION

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring 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.

Other Important Information: You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by 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 a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 2000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfc_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

This notice was not delayed by a law enforcement investigation.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfc_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).