

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

KATHLEEN A. MONAGHAN, ESQ.
KMonaghan@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Visit us online at
www.C-WLAW.com

Phone: (610) 567-0700

Fax: (610) 567-0712

CONFIDENTIAL ATTORNEY
WORK PRODUCT

March 3, 2025

Via Email

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

RE: Data Security Notification

To Whom It May Concern:

We serve as counsel for Apache Mills Inc. ("Apache Mills") located at 417 S River Street, Calhoun, Georgia 30701. We write to provide notification of a recent data security incident. By providing this notice, Apache Mills does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or about August 17, 2024, Apache Mills Inc. ("Apache Mills") experienced a network disruption that impacted its ability to access certain systems. Upon discovery, Apache took immediate action to address and investigate the event, which included contacting law enforcement and engaging third-party specialists to assist with determining the nature and scope of the event. A thorough investigation determined that certain information was accessed by an unauthorized actor from August 13, 2024, to August 17, 2024. Apache Mills then undertook a comprehensive and time-consuming review of the potentially impacted data in order to determine the type(s) of information contained within the dataset and to whom that information related. Once this review was completed, Apache Mills immediately worked to obtain up-to-date address information in order to provide potentially impacted individuals with notice.

On or about January 23, 2025, Apache Mills completed its review of the data, which included obtaining address information for the potentially impacted individuals. On February 25, 2025, a National Change of Address search was conducted, and it was determined that information related to one (1) Maryland resident may have been impacted. The information believed to be at risk includes first and last name, in combination with a Social Security number and health insurance information.

In response to this incident, Apache Mills immediately took steps to secure its network environment and undertook a thorough investigation. Apache Mills has also implemented additional technical safeguards to further enhance the security of information in its possession and to prevent similar events from happening in the future. Additionally, Apache Mills began providing notice to the potentially impacted individuals on March 03, 2025 via U.S. mail. A copy of the notice is attached hereto as *Exhibit A*. While Apache Mills has no reason to believe any information has been misused as a result of this incident; in an abundance of caution, Apache Mills is offering the potentially impacted individuals 12 months of complimentary credit monitoring and identity protection services.

Very truly yours,

CIPRIANI & WERNER, P.C.

By:

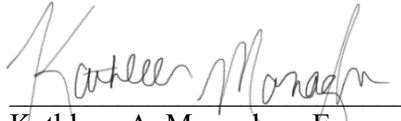

Kathleen A. Monaghan, Esq.

Exhibit “A”

Apache Mills, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



P



March 3, 2025

Dear [REDACTED]:

We write to inform you of a data security incident experienced by Apache Mills, Inc. ("Apache Mills") that may have involved your information as described below. We take the privacy and security of all information very seriously and are providing information about the incident and steps you can take to help protect your information.

What Happened: On or around August 17, 2024, Apache Mills experienced a network disruption that impacted our ability to access certain systems. Upon discovery, we immediately took action to address and investigate the event, which included contacting law enforcement and engaging third-party computer forensic specialists to assist with determining the nature and scope of the event. A thorough investigation determined that certain information was accessed by an unauthorized actor from August 13, 2024, to August 17, 2024. We then began a comprehensive and time-consuming review of the potentially impacted data in order to determine the type(s) of information contained within the dataset and to whom that information related. Once this review was completed, we began working to obtain up-to-date address information in order to provide you with this notice. That process was completed on January 23, 2025, and we worked to provide you with this notification as soon as possible.

What Information Was Involved: The types of information that may have been contained within the affected emails includes your first and last name, in combination with: [REDACTED]. Please note that we currently have no reason to believe that your information has been or will be misused as a result of this event.

What We Are Doing: We have taken the steps necessary to address the incident and are committed to fully protecting all of the information that you have entrusted to us. Upon learning of this incident, we immediately took steps to secure the environment and undertook a thorough investigation. We also implemented additional technical safeguards to further enhance the security of information in our possession and to prevent similar incidents from happening in the future. Additionally, we are offering you complimentary credit monitoring and identity protection services.

What You Can Do: We recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports, account statements, and explanations of benefits forms for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft, including activating the complimentary credit monitoring and identity protection services we are offering.

000010102G0500

P

For More Information: Should you have any questions or concerns, our dedicated call center can be reached at 1-833-799-3897 from 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays. Representatives are available for 90 days from the date of this letter. The security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support during this time.

Sincerely,

A handwritten signature in black ink, appearing to be 'Lee Gentry', with a long horizontal line extending to the right.

Lee Gentry
Chief Financial Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.



To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

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

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

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
--	--	---

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. 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; 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Apache Mills, Inc. may be contacted at 197 Royal Drive, Calhoun, GA 30701.

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.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island resident impacted by this incident.