



ROPE & GRAY LLP
PRUDENTIAL TOWER
800 BOYLSTON STREET
BOSTON, MA 02199-3600
WWW.ROPEGRAY.COM

August 9, 2023

BY EMAIL

Attorney General John Formella
Consumer Protection & Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Associated Materials Data Incident

Dear General Formella:

We are legal counsel to Associated Materials, LLC (“Associated Materials” or the “Company”), a manufacturer and distributor of exterior building products headquartered in Ohio. We are writing to notify your office about an incident involving potential unauthorized access to the personal information of approximately one New Hampshire resident.

On May 12, 2023, Associated Materials became aware of service outages at one of its manufacturing plants and, upon further investigation, discovered that certain systems had been encrypted by an unauthorized party. Associated Materials promptly engaged experts and commenced an investigation to determine the extent of any unauthorized activity and identify the files that may have been accessed and copied by the unauthorized party. The investigation revealed that the unauthorized activity likely took place between approximately April 25, 2023, and May 12, 2023. Given that the files were encrypted, the process of reviewing the files to determine what personal information may have been involved was a lengthy and complex process.

Associated Materials’ review identified personal information about principally employees and former employees within the documents. The personal information identified varies by individual but may have included for the New Hampshire resident the individual’s

Associated Materials is not aware of any misuse of the information as a result of this incident. Nevertheless, Associated Materials sent notifications by mail on August 8, 2023 to the individuals whose information was identified as contained in the files. The notification includes a premier credit monitoring and identity theft protection product free of charge. Additional information on the identity protection services is included in the attached sample of the notification.

ROPES & GRAY LLP

Attorney General Formella

- 2 -

August 9, 2023

Upon discovering the incident, Associated Materials promptly investigated and implemented additional measures designed to increase the security of its network, including by changing the passwords on the affected systems and implementing other access controls. Associated Materials notified law enforcement, including the Federal Bureau of Investigation.

If you have any questions, please do not hesitate to contact me at _____ or _____

Respectfully,

Kevin J. Angle

Enclosure: Form of Individual Notice



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

<<Date>>

Notice of Data Breach

Dear _____ :

We are writing to share information with you regarding a recent security incident that may have involved files containing your personal information. While we are not aware of any actual or attempted misuse of the information, we are providing you with information about the event, our thorough response, and additional measures you can take if you wish to do so.

What Happened?

On May 12, 2023, we became aware of service outages at one of our manufacturing plants. Upon further investigation, the Associated Materials information technology team discovered that certain systems had been encrypted by an unauthorized party. We promptly engaged external counsel and a leading third-party cybersecurity forensics firm to investigate the extent of any unauthorized activity and identified files that may have been accessed and copied by the unauthorized party. Based on the results of our investigation, it appears that the activity of the unauthorized party occurred between approximately April 25, 2023, and May 12, 2023. Given that the files were encrypted, the process of reviewing the files to determine what personal information may have been involved was lengthy and a complex process. Through our review, we identified some of your personal information as contained in the files that may have been accessed and copied. While the unauthorized party potentially had access to and copied your information, we want to reiterate that we are not aware of any fraudulent activity associated with it.

What Information Was Involved?

Some of the files that may have been accessed and copied contained personal information about you. The information contained in the files may include your

What We Are Doing.

We promptly investigated to determine the scope of any unauthorized access to our systems, notified law enforcement, and, following our investigation, implemented additional measures designed to increase the security of our network, including by changing the passwords on the affected systems and implementing other access controls. Since these efforts, we have not observed any further unauthorized activity.

What You Can Do.

As you should always do, we recommend you watch for any unusual emails or messages. You should confirm that any request to click a link, download something, or provide sensitive personal information is legitimate.

Although we are not aware of any fraudulent activity associated with your personal information, it is always advisable to regularly review your financial accounts and report any suspicious or unrecognized activity. The enclosed “General Information About Identity Theft Protection” provides further information about steps that you can take. Federal regulatory agencies recommend vigilance for the next and that you report any suspected incidents of fraud to the relevant financial institution immediately. Furthermore, the Federal Trade Commission provides a wealth of advice and recommendations for consumers on how to protect themselves from and respond to identity theft in the event that such information is needed.

Other Important Information.

In order to assist you with this vigilance, arrangements have been made to provide you with a membership in Equifax’s Credit Watch Gold credit monitoring product at no cost to you. Details about this offer and your activation code are included in the enclosed form. While we hope that this service provides some peace of mind, the opportunity to subscribe to these services is not intended to suggest that you are at risk of harm.

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Equifax Credit Watch Gold online, or have other questions about this matter please contact , Monday through Friday, 9:00 AM to 9:00 PM Eastern Time.

We regret this incident. Please be assured that we are working hard to prevent this type of security matter from occurring in the future.

Sincerely,

James Drexinger
Chief Executive Officer



Enter your Activation Code
Enrollment Deadline:

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 notifications¹ 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 alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- 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 theft⁴

Enrollment Instructions

Go to

Enter your unique Activation Code of
these 4 steps:

then click “Submit” and follow

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.

¹WebScan 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.²The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.³Locking 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.com⁴The 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.

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

It is always advisable to regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com by calling toll free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below:

- **Equifax**, P.O. Box 740241, Atlanta, Georgia 30374-0241. 1.800.685.1111. www.equifax.com
- **Experian**, P.O. Box 9532, Allen, TX 75013. 1.888.397.3742. www.experian.com
- **TransUnion**, 2 Baldwin Pl., P.O. Box 1000, Chester, PA 19016. 1.800.916.8800. www.transunion.com

Fraud Alert: You may contact the fraud department of the three major credit bureaus to request that a “fraud alert” be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

Equifax:	Report Fraud:	1.800.685.1111
Experian:	Report Fraud:	1.888.397.3742
TransUnion:	Report Fraud:	1.800.680.7289

Security Freeze for Credit Reporting Agencies: You may request a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer’s credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. It is free to place, lift or remove a security freeze. You must separately place a security freeze on your credit report at each credit bureau. To do so, you must contact the credit bureaus by phone, mail, or secure electronic means:

- **Equifax:** P.O. Box 105788, Atlanta, GA 30348, 1.800.349.9960, www.Equifax.com
- **Experian:** P.O. Box 9554, Allen, TX 75013, 1.888.397.3742, www.Experian.com
- **TransUnion:** P.O. Box 2000, Chester, PA 19106, 1.888.909.8872, www.TransUnion.com

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.),
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

If you request a freeze online or by phone, the agency must place the freeze within one business day. The credit bureaus have three business days after receiving a request by mail to place a security freeze on your credit report, and they must also send confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the freeze to allow a specific entity or individual access to your credit report, you must contact the credit reporting agencies and include (1) proper identification; (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available.

You also have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/documents/bcfc_consumer-rights-summary_2018-09.pdf or www.ftc.gov.

Steps You Can Take if You Are a Victim of Identity Theft

- **File a police report.** Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- **Contact the U.S. Federal Trade Commission (FTC).** The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); online at <http://www.ftc.gov/idtheft>; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.
- **Keep a record of your contacts.** Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is helpful to log conversations with creditors, law enforcement officials, and other relevant parties.

Additional Steps to Avoid Identity Theft: The FTC has further information about steps to take to avoid identity theft at: <http://www.ftc.gov/idtheft>; calling 1-877-IDTHEFT (438-4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

State Specific Information

District of Columbia residents may contact the District of Columbia Attorney General at 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and <https://oag.dc.gov/>.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling (515) 281-5926 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, calling the Identity Theft Unit at 1.410.576.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above and you have rights under the Fair Credit Reporting Act as described above.

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

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/>, calling 1.919.716.6000 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (503) 378-4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government- issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 1.410.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at <https://ago.vermont.gov/>.