



<<Date>>

<<Name>>

<<Street Address>>

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

Dear <<Name>>:

Huntsman Building Solutions (USA) LLC ("HBS" or the "Company") is committed to protecting your personal information. Unfortunately, we recently learned that HBS was the victim of a security incident impacting certain files on the Company's information systems. We are sending you this letter to provide information about the incident and to share the steps that HBS has taken to address it.

On February 11, 2025, we learned that an unauthorized third party had gained access to our information systems. The Company's IT team immediately blocked any further access by the unauthorized third party, took steps to ensure our systems are secure and commenced a comprehensive investigation with the assistance of a leading cybersecurity firm. After a lengthy and thorough analysis of this incident, we were able to determine that your personal information including your name and <<Categories of Data>> potentially was compromised.

**We have no evidence that your personal information has been, or will be, misused.**

Nevertheless, as a precautionary measure, the Company is offering you 24 months of credit monitoring and identity protection services, at no cost to you. These services, through Privacy Solutions, provide credit monitoring through Equifax, credit report and score access, identity theft insurance, identity restoration services, and dark web monitoring.

To enroll in the credit monitoring and identity protection services at no charge, please visit [www.privacysolutions.com](http://www.privacysolutions.com) and enter the following activation code, <<Activation Code>>, to activate your membership and start monitoring your personal information. Please note the deadline to enroll is 60 days from the date of this letter.

In addition to the offer of credit monitoring and identity protection services, we have provided with this letter information on steps you can take to protect the security of your personal information. We urge you to carefully review this information.

HBS takes this incident very seriously, and we have already taken steps to prevent a recurrence. We also have reported this incident to law enforcement and are cooperating with the investigation.

We regret any inconvenience this incident may cause you. Should you have any questions or concerns regarding this incident, please email us at [HBSdatabreach@huntsman.com](mailto:HBSdatabreach@huntsman.com), or call us toll free at 1-855-761-0067, extension 90004.



Sincerely,

A handwritten signature in black ink, appearing to read "Doug Brady". The signature is fluid and cursive, with the first name "Doug" and last name "Brady" clearly distinguishable.

Doug Brady  
VP, Huntsman Building Solutions, Global  
Huntsman Building Solutions (USA) LLC



### **Steps to Protect the Security of Your Personal Information**

By taking the following steps, you can help reduce the risk that your personal information may be misused.

**1. Enroll in Credit Monitoring and Identity Protection Services.** You must personally activate the credit monitoring and identity protection services for it to be effective. To activate your membership please visit [www.privacysolutions.com](http://www.privacysolutions.com) and enter the activation code contained in the notice letter. Your 24-month membership in Privacy Solutions provides credit monitoring through Equifax, credit report and score access, identity theft insurance, ID Restoration services, and dark web monitoring.

**2. Review your credit reports.** You are entitled to a free copy of your credit report from each of the three national credit bureaus once a week. To obtain a free credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 877-322-8228. You can also receive free credit reports by placing a fraud alert, described below. Errors in your credit report, such as a home address or accounts you do not recognize, may be a sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your credit report, whether or not due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected.

**3. Review your account statements.** Although we have no reason to believe that your payment or other financial information was impacted by this incident, you should carefully review statements that you receive from credit card companies, banks, utilities and other services for suspicious activity.

**4. Remain vigilant and respond to suspicious activity.** If you notice suspicious activity on an account statement, report it to your credit card company or service provider and consider closing the account. You should also consider reporting such activity to the Company, your local police department, your state's attorney general and the Federal Trade Commission.

**5. You have the right to place a "security freeze" on your credit report.** A security freeze will restrict access to your credit file, by prohibiting a consumer reporting agency from releasing information in your credit file without your consent. This will prevent any unauthorized individuals from opening new credit, loans, or other accounts in your name. However, placing a security freeze on your credit file can delay or make it more difficult for you to request or apply for a new loan, mortgage or any other account involving the extension of credit. A security freeze does not apply to existing accounts you have that request information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases and account upgrades and enhancements.

There is no charge to place a security freeze. Do not confuse security freezes with "credit locks" or similar programs—although they work in similar ways, credit locks typically come with monthly fees or other expenses. If you want to freeze your credit for free, as guaranteed by federal law, then opt for a security freeze and not a credit lock.

To place a security freeze on your credit file, contact all three of the nationwide credit bureaus, listed below, either online, by mail or by phone. You will need to provide appropriate proof of your identity, including your name, address, date of birth, Social Security number and other personal



information. After receiving your freeze request, each bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. The contact information for all three credit bureaus is:

Equifax  
P.O. Box 105788  
Atlanta, GA 30348  
1-888-378-4329  
[www.equifax.com](http://www.equifax.com)

Experian  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 160  
Woodlyn, PA 19094  
1-800-916-8800  
[www.transunion.com](http://www.transunion.com)

**6. Consider placing a fraud alert with one of the three nationwide credit bureaus.** You can place an initial fraud alert by contacting one of the three nationwide credit bureaus listed above. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit bureaus listed above. As soon as that bureau processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file.

An initial fraud alert stays in your file for at least one year. To place this alert, a credit bureau will require you to provide appropriate proof of your identity, which may include your Social Security number. An initial fraud alert entitles you to a copy of all the information in your file at each of the three nationwide credit bureaus listed above. These additional disclosures may help you detect signs of fraud, for example, whether fraudulent accounts have been opened in your name or whether someone has reported a change in your address. If you are the victim of identity theft, you are entitled to an extended fraud alert, which lasts seven years.

**7. Additional Information.** You may obtain additional information about fraud alerts, security freezes and steps you can take to avoid identity theft from the following: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; [www.ftc.gov/idtheft/](http://www.ftc.gov/idtheft/); (877) IDTHEFT (438-4338).



**If you live in Maryland, please read the additional notice below that applies to you:**

You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft. The Attorney General Office may be contacted as follows:

Office of the Attorney General  
200 St. Paul Place  
Baltimore, MD 21202  
1-888-743-0023  
[www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov)

**If you live in Massachusetts, please read the additional notice below that applies to you:**

Massachusetts law gives you right to report this incident to the police in the county where you reside and to receive a police incident report within 24 hours of filing.

**If you live in New Mexico, please read the additional notice below that applies to you:**

Please visit the following link to review a summary of your major rights under the federal Fair Credit Reporting Act (FCRA): [https://files.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf).

**If you live in New York, please read the additional notice below that applies to you:**

You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft. The Attorney General Office may be contacted as follows:

Office of the Attorney General  
The Capitol  
Albany, NY 12224-0341  
1-800-771-7755  
[www.ag.ny.gov/](http://www.ag.ny.gov/)

**If you live in North Carolina, please read the additional notice below that applies to you:**

You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft. The Attorney General Office may be contacted as follows:

North Carolina Office of the Attorney General  
Consumer Protection Division  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
919-716-6000  
[www.ncdoj.gov](http://www.ncdoj.gov)