



April 15, 2024

Re: Notice of Data Breach

Dear [Name]:

Crossmark, Inc. (the “Company”) values its employees and takes seriously our obligation to protect your personal information. We are writing to inform you of a recent incident involving your personal information. At the outset, I want to make clear that we do not believe your personal information has been misused, compromised, or remains accessible to any unauthorized individual as a result of this incident. We are sending you this letter because we deem it important to keep you apprised of any incident involving your personal information.

What Happened?

On March 15, 2024, the Company learned that an employee in our Human Resources (HR) Department inadvertently attached a spreadsheet containing your personal information (the “Attachment”) to an email sent to Company District Managers. Immediately after sending the email the employee realized their mistake and notified the Company of the issue. The Company’s Information Technology department then immediately took steps to delete the email from the Company’s servers, and the email accounts of the employees who received the attachment.

What Information Was Involved?

The Attachment contained your name and Social Security number. As mentioned above, the Company has taken steps to ensure that both the Attachment and the email were permanently deleted from the recipient employees’ email accounts. We also contacted each of the employees who received the Attachment to confirm their deletion. Based on all of this, we do not believe that your personal information has been misused in any way as a result of this event.

What We Are Doing?

The Company is offering you one year of identity protection services, at no cost to you, through Experian, one of the three nationwide credit bureaus. Your one-year membership in Experian’s



IdentityWorksSM product provides identity restoration services, fraud detection tools, and other benefits, which include monitoring your credit file at Experian.

What You Can Do

You can call Experian's identity restoration agents to assist you to investigate and resolve any incidents of fraud. You may take advantage of this benefit, at any time, until July 31, 2025, by calling Experian at 1-877-890-9332. No enrollment or activation is necessary. The terms and conditions for identity restoration are located at: www.ExperianIDWorks.com/restoration.

While identity restoration is immediately available to you, you may also activate the fraud detection tools available through IdentityWorksSM. This product provides you with identity detection, credit monitoring, and resolution of identity theft. If you wish to enroll in IdentityWorksSM, you will need to do the following:

1. Visit the IdentityWorksSM web site: www.experianidworks.com/credit or call 1-877-890-9332 to enroll and provide Engagement Number **B120337**
2. PROVIDE your Activation Code: **V8WQ5Y6D6**

Enrollment Deadline: July 31, 2024 (your Activation Code will not work after this date).

If you have any questions concerning IdentityWorksSM, or if you prefer to enroll over the phone for delivery of your membership via U.S. mail, please call Experian at 1-877-890-9332. Be prepared to provide Engagement Number B120337 as proof of eligibility for the identity protection product by Experian. Although we do not believe there is any risk to your information as a result of this event, we have also included with this letter additional information on steps you can take to protect the security of your personal information.

Other Important Information

The Company is taking all of the necessary steps to ensure that this does not happen again.

For More Information

Should you have any questions or concerns, please do not hesitate to contact Chris Ponder II, VP Human Resources, 469.971.4319.



Sincerely,

Chris Ponder II
VP Human Resources
Crossmark, Inc.

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 IdentityWorksSM. You must personally activate identity monitoring for it to be effective. The notice letter contains instructions and information on how to activate your IdentityWorksSM membership. Experian's IdentityWorksSM product will provide the following:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors your credit files at Experian for indicators of fraud.
- **Identity Restoration:** Identity restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorksSM ExtendCARE:** You will receive the same high level of identity restoration support even after your IdentityWorksSM membership expires.
- **\$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Please direct questions about the IdentityWorksSM product to Experian. A credit card is not required for enrollment in IdentityWorksSM. Enrollment in IdentityWorksSM will not affect your credit score. The Terms and Conditions for this offer are located at: www.ExperianIDWorks.com/restoration.

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 annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You can also receive free credit reports by placing a fraud alert, described below. Errors in information 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 none of your payment or other financial information was impacted by this incident, you should carefully review for suspicious

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² 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.

activity the statements that you receive from credit card companies, banks, utilities, and other services.

4. Remain vigilant and respond to suspicious activity. If you receive an e-mail or mail alert from Experian, contact an IdentityWorksSM identity resolution agent toll-free at 1-877-890-9332 or visit www.ExperianIDWorks.com/restoration for additional information. You should consider changing your username, passwords, security questions, and security answers to your online accounts. 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 express 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 may also 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. Don't confuse security freezes with “credit locks” or similar programs—they work in similar ways, but 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 to the credit bureau, which will include your name, address, date of birth, Social Security number, and other personal information. After receiving your freeze request, each credit 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 as follows:

Equifax
P.O. Box 105788
Atlanta, GA 30348
1-888-685-1111

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 2000
Woodlyn, PA 19094
1-888-909-8872

www.equifax.com

www.experian.com

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. If you are the victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. 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.

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

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

Law enforcement has not requested that we delay notifying you.

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/documents/bcfc_consumer-rights-summary_2018-09.pdf.