



CROSSROADS

March 25, 2025

Via E-Mail

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

To Whom It May Concern:

I am writing on behalf of Crossroads Trading Co., Inc. ("Crossroads" or the "Company") to inform you of a security incident that may impact 185 Maryland residents.

On February 15, 2025, an unauthorized third-party gained access to our server and subsequently encrypted data stored on the Company's network. The Company's IT team immediately responded to the incident and was able to swiftly secure our network, restore systems, and prevent further access by the third-party. Crossroads retained a team of expert forensic investigators and performed a comprehensive investigation, which confirmed that the third-party's access was limited to a segment of our network. Crossroads also retained a cyberthreat firm and took affirmative steps to prevent the encrypted data from being published, distributed, or misused.

The Company's investigation determined that the data encrypted by the unauthorized third party contained the personal information of Maryland residents, including name, Social Security number, and driver's license or state ID number.

Please note that we have received no information indicating that the personal information of the Maryland residents has been, or will be, published or otherwise misused. The Company notified its employees by email of this incident on February 26, 2025, as a voluntary, proactive measure. Nevertheless, we have notified all potentially impacted Maryland residents on March 25, 2025, and offered them two years identity theft protection services, paid for by Crossroads. A template copy of the notification sent to Maryland residents is attached to this letter.

We have also contacted the Federal Bureau of Investigation regarding this incident, and have cooperated in their investigation.

If you have any questions concerning this matter, please do not hesitate to contact our counsel Mr. Kwabena Appenteng at Kappenteng@littler.com, and Mr. Andrew Gray at Argray@littler.com.

Very truly yours,

Aruna Busacca

Aruna Busacca
Chief Operating Officer
Crossroads Trading Co., Inc.



CROSSROADS

Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[NAME]
[STREET]
[CITY], [STATE] [ZIP CODE]

[DATE]

Dear [NAME]:

Crossroads Trading Co., Inc. ("Crossroads" or the "Company") takes seriously its obligation to safeguard the personal information of our customers. Unfortunately, Crossroads recently learned that it was the victim of a security incident. We are writing to provide you with information about the scope of the incident and share with you the steps that Crossroads is taking to address it.

On February 15, 2025, an unauthorized third-party gained access to our server and encrypted data stored on the Company's network. The Company's IT team immediately responded to the incident and was able to swiftly secure our network, restore systems, and prevent further access by the third-party. Crossroads retained a team of expert forensic investigators and performed a comprehensive investigation, which confirmed that the third-party's access was limited to a segment of the Company's network. Crossroads also engaged a cyberthreat firm and took affirmative steps to prevent the encrypted data from being published, distributed or misused.

We have no evidence that your personal information has been, or will be, misused or published. Nevertheless, we are notifying you because our investigation has determined that the encrypted data included at least one document that contained your name and [CATEGORIES OF DATA].

As a precautionary measure, the Company is offering you two years of identity protection services through Experian, at no cost to you. This two-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.

You can call Experian's identity restoration agents to assist you in investigating and resolving any incidents of fraud. You may take advantage of this benefit, at any time within the next two years by calling Experian at 833-918-6165. 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 IdentityWorks. This product provides you with identity detection, credit monitoring, and resolution of identity theft. If you wish to enroll in IdentityWorks, you will need to do the following:

- Ensure that you **enroll by 06/30/2025** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: **[ACTIVATION CODE]**

If you have questions about IdentityWorks, need assistance with identity restoration, or would prefer to enroll in IdentityWorks by telephone, please contact Experian's customer care team at 833-918-6165 by **06/30/2025**. Be prepared to provide engagement number **[NUMBER]** as proof of eligibility for these services from Experian.

In addition to the offer of identity protection services, enclosed is information on the steps you can take to protect the security of your personal information. We urge you to carefully review this information.

Crossroads takes this incident very seriously and we have already taken steps to prevent a recurrence. We have also reported this incident to and met with the FBI, and we are continuing to cooperate in the FBI's investigation.

The Company regrets this incident and any inconvenience it may have caused you. Should you have any questions or concerns regarding this incident, our call center is available to assist you at [PHONE NUMBER] between 8 AM and 8 PM (CST) / 6 AM and 6 PM (PST), Monday through Friday.

Sincerely,

Aruna Busacca

Aruna Busacca
Chief Operating Officer
Crossroads Trading Co., Inc.

CROSS-ADT-CST-CM

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 IdentityWorks. You must personally activate identity monitoring for it to be effective. The notice letter contains instructions and information on how to activate your IdentityWorks membership. Experian's IdentityWorks 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 only¹.
- **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 IdentityWorks ExtendCARE:** You will receive the same high level of identity restoration support even after your IdentityWorks membership expires.
- **\$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Please direct questions about the IdentityWorks product to Experian. A credit card is not required for enrollment in IdentityWorks, and enrollment will not affect your credit score.

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 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 receive an e-mail or mail alert from Experian, contact an IdentityWorks identity resolution agent toll-free at 833-918-6165 or visit www.ExperianIDWorks.com/restoration for additional information. 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.

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.

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

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

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-800-916-8800
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/; (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

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.

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/

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

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

Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

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:

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
401-274-4400
www.riag.ri.gov

[NUMBER] Rhode Island residents are potentially affected by this security incident.

If you live in Washington D.C., please read the additional notice below that applies to you:

You can obtain information from the D.C. Attorney General about steps you can take to prevent identity theft. The Attorney General Office may be contacted as follows:

District of Columbia Attorney General
400 6th Street, NW, Washington, DC 20001
202-727-3400
www.oag.dc.gov

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

We have not delayed notifying you at the request of law enforcement.