



Dear [REDACTED]

We are writing with important information regarding a recent data security incident at Brox Industries, Inc. (“Brox Industries”) that may involve some of your personal information. We wanted to provide you with information about the incident at Brox Industries, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your personal information.

Upon learning of the issue, we promptly contained the incident and commenced an immediate and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive investigation and manual document review, we discovered on or about October 3, 2025, that files containing your personal information may have been impacted as a result of the incident, including your first and last name, and [REDACTED]

We have no evidence of any identity theft or financial fraud directly resulting from this incident. Out of an abundance of caution to protect yourself from potential misuse of their information, we are offering complimentary access to identity monitoring for 24-months. For more information on identity theft prevention and the identity-monitoring product being offered to you, including instructions on how to activate your complimentary 24-month membership, please see the additional information provided in this letter.

This letter provides precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze your credit files, and or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. To the extent that it is helpful, we are also suggesting steps you can take to protect your medical information. For more information and instructions on how to activate the credit monitoring product being offered to you, please review the “Other Important Information” section.

Brox Industries values your privacy and deeply regrets that this incident has occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. Since detecting the incident, we have reviewed and revised our information security practices and implemented additional security measures to mitigate the chance of a similar event in the future.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have established to respond to questions surrounding the incident at (866) 291-1760.

This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9:00 am to 6:30 pm Eastern Time, excluding holidays.

Sincerely,

Brox Industries, Inc.

One Tech Drive, Suite 310
Andover, MA 01810

OTHER IMPORTANT INFORMATION

1. Enrolling in Complimentary 24-Month Credit Monitoring

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until [REDACTED] to activate your identity monitoring services.

Membership Number: [REDACTED]

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you chose to use the complementary monitoring services, we recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian

P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC

P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
<https://www.freeze.equifax.com>
1-800-349-9960

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016
<http://www.transunion.com/securityfreeze>
1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing 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.

If you do place a security freeze *prior* to enrolling in any credit monitoring service, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Protecting Your Medical Information.

As a general matter the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits" statement which you receive from your health insurance company. Follow up with your insurance company or the care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential disclosure (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or care provider for any items you do not recognize.

6. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve yourself of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report 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.