123 South Front Street, Memphis, TN 38103 Phone (901) 495-6500

DOUGLAS BALDWIN
Chief Information Security Officer
Customer Satisfaction

November 20, 2023

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
consumer@ag.iowa.gov

Dear Attorney General Brenna Bird,

We are writing to notify you of a data security incident involving a third-party secure file transfer application, MOVEit Transfer, used by our company, AutoZone, Inc. ("AutoZone"). This incident involved personal information maintained by AutoZone related to 654 Iowa residents. At this time, we have no indications that the personal information has been subject to fraud as a result of this incident.

AutoZone became aware that an unauthorized third party exploited a vulnerability associated with MOVEit and exfiltrated certain data from an AutoZone system that supports the MOVEit application. As has been widely reported, over two thousand organizations around the world were impacted by the vulnerability in the MOVEit Transfer application. Upon becoming aware of this situation, AutoZone commenced an investigation, retained outside experts, and took measures to assess and remediate the incident. More specifically, on or about August 15, 2023, AutoZone determined that the exploitation of the vulnerability in the MOVEit application had resulted in the exfiltration of certain data. We have no evidence at this time that the incident is ongoing.

We also conducted a review of the data that was acquired by the threat actor, which was completed as of November 3, 2023. Based on that review, we determined that the personal information of 654 Iowa residents was impacted. A sample individual notice is enclosed, which will be sent to each impacted individual. The potentially impacted information includes the individual's name with Social Security Number and in some instances date of birth.

As an added precaution, AutoZone is offering the potentially impacted individuals complimentary access to twelve (12) months of credit monitoring services through Equifax.

Sincerely,

Douglas Baldwin
Chief Information Security Officer
AutoZone, Inc.

Return Mail Processing
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

DOUGLAS BALDWIN
Chief Information Security Officer
Customer Satisfaction

<<Variable Header>>

Dear <<Name 1>>,

We are writing to notify you of an incident involving a third-party secure file transfer application, MOVEit, used by AutoZone, Inc. ("AutoZone"). We have determined that this incident, which has been contained, impacted your personal information. At this time, we are not aware that your personal information has been subject to fraud resulting from this incident. We are notifying you to explain the circumstances and to inform you of the steps we have taken and the resources we are making available to you.

What Happened?

AutoZone became aware that an unauthorized third party exploited a vulnerability associated with MOVEit and exfiltrated certain data from an AutoZone system that supports the MOVEit application. As has been widely reported, over two thousand organizations around the world were impacted by the vulnerability in the MOVEit Transfer application. Upon becoming aware of this situation, AutoZone commenced an investigation, retained outside experts, and took measures to assess and remediate incident. We have performed an analysis of the affected system and associated data to determine whether your information was potentially impacted. More specifically, on or about August 15, 2023, AutoZone determined that the exploitation of the vulnerability in the MOVEit application had resulted in the exfiltration of certain data. Based on that analysis, we have determined that certain of your information was included in those files.

What Information Was Involved?

Based on our investigation, we understand that your <<Breached Elements>> were obtained by an unauthorized third party.

What We Are Doing.

Upon becoming aware of the incident, we began an investigation to understand the scope and impact. We also took measures to address the vulnerability, including temporarily disabling the MOVEit application, rebuilding the affected system, and patching the vulnerability. We have no evidence at this time that the incident is ongoing.

What You Can Do.

As a reminder, at this time, we are not aware that your personal information has been subject to fraud as a result of this incident. Nevertheless, we recommend that you remain vigilant for fraud and identity theft.

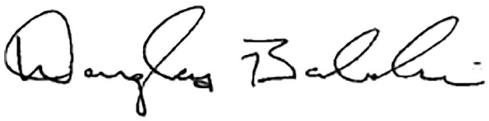
We encourage you to review and monitor your account for suspicious activity. Federal regulatory agencies recommend that you remain vigilant for the next 12 to 24 months and report any suspected incidents of fraud to us or the relevant financial institution. We would also encourage you to avoid clicking on links or downloading attachments from suspicious emails and to be cautious of any unsolicited communications that ask for your personal information or refer you to a website asking for personal information. Please refer to the enclosure entitled "Additional Ways to Protect Your Identity" for additional actions you should consider taking to protect yourself against fraud and identity theft.

Finally, as an additional safeguard, we have arranged for you to enroll, at no cost to you, in an online identity monitoring service for <<CM Length>> months of credit monitoring and identity protection services through Equifax. Due to State and Federal privacy laws, however, we cannot enroll you directly and if you wish to take advantage of this complimentary credit monitoring service, you must enroll yourself.

For More Information.

If you have additional questions, please contact us at 877-554-4891, from 8:00 a.m. to 8:00 p.m. Central, Monday through Friday, excluding holidays.

Sincerely,



Douglas Baldwin
Chief Information Security Officer
AutoZone, Inc.

EQUIFAX®

<<Name1>>
Enter your Activation Code: <<*ACTIVATIONCODE*>>
Enrollment Deadline: <<*ENROLLMENTDEADLINE*>>

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product.

Key Features

- Annual access to your 3-bureau credit report and VantageScore[1] credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring[2] with email notifications of key changes to your credit reports
- WebScan notifications[3] 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 alerts[4], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[5]
- 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 theft[6]
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit, and personal identification cards

Enrollment Instructions

Go to ***www.equifax.com/activate***
Enter your unique Activation Code of <<*ACTIVATIONCODE*>>, then click "Submit" and follow these 4 steps:

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.

---

[1] The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

[2] Credit monitoring from Experian and TransUnion will take several days to begin.

[3] WebScan 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.

[4] The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[5] Locking 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.com.

[6] The 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.

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity. Here are some we suggest you consider:

Reviewing Your Accounts and Credit Reports

Regulators recommend that you be especially vigilant for the next 12 to 24 months. As part of staying vigilant, you should regularly review your account statements, and periodically obtain your credit report from one or more of the three national credit reporting companies. Those companies are:

Equifax 1-800-525-6285 Equifax.com	**Experian** 1-888-397-3742 Experian.com	**TransUnion** 1-800-680-7289 Transunion.com

You can obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report 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. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert

A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report.

If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report

A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will provide you a PIN number or a password when you place a security freeze. You will need that PIN or password to lift the freeze, and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft

If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

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. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and file a complaint online at www.IdentityTheft.gov. You can also file a complaint by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of *Identity Theft: A Recovery Plan*, a guide from the FTC to help you guard against and deal with identity theft. It is available online at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, or unverifiable information. You can find more information about your rights under the FCRA online at www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

Special Information for Residents of the District of Columbia, Iowa, Maryland, Massachusetts, New Mexico, New York, North Carolina, Oregon, Rhode Island, and Vermont.

District of Columbia residents can learn more about preventing identity theft from the District of Columbia Office of the Attorney General, by visiting their website at https://oag.dc.gov/, calling (202) 727-3400, or requesting more information via email oag@dc.gov or mail 400 6th Street NW, Washington DC 20001.

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) 281-5164 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 http://www.oag.state.md.us/idtheft/index.htm, calling the Identity Theft Unit at 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. There is no charge to place a security freeze on your account; however, you may be required to provide the credit reporting agency with 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 its honoring your request.

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 obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

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 1.919.716.6400 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. You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

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 http://www.atg.state.vt.us.