October 9, 2024

<u>BY EMAIL</u>

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,

Lowe's Companies, Inc ("Lowe's") is providing this notice of a cybersecurity event to your office pursuant to Md. Code Ann., Com. Law § 14-3504(h).

On September 2, 2024, Lowe's detected unauthorized third-party access to certain employee's online Workday accounts. Workday is a third-party provider that supports some of Lowe's HR applications. Upon detecting the unauthorized access, Lowe's promptly activated its incident response procedures and launched an investigation into the nature and scope of the incident.

Lowe's investigation into the incident concluded on September 9, 2024. Lowe's investigation revealed that an unauthorized third party likely obtained a limited number of employees' Workday usernames and passwords through a phishing campaign involving Google advertisements with fraudulent Lowe's Workday domain addresses. Upon obtaining the employee's Workday credentials, the threat actor gained temporary access to those employees' Workday accounts. We have no evidence that Lowe's own systems or network environment were affected by this incident.

On September 9, 2024, Lowe's determined that 13 residents of Maryland were affected by this incident. The threat actor was able to view the following information after gaining access to the affected employee's Workday accounts: first and last name, bank account number, date of birth, address, email address, and phone number.

Lowe's notified all affected employees via email on September 6, 2024. Lowe's began sending affected employees formal notice on October 9, 2024 via U.S. mail. Attached is a copy of the employee notification mailed to the affected individuals in Maryland. Lowe's is offering affected employees with 12 months of complimentary credit monitoring and identity theft protection services through Experian.

Lowe's promptly took steps to remediate the unauthorized access and to avoid similar activity in the future. Specifically, Lowe's reset Workday passwords for all impacted employees, temporarily disabled the ability to make payment elections changes off Lowe's network, and temporarily disabled access to Workday from outside of the Lowe's network. Lowe's is also expediting its ongoing implementation of an MFA solution for Workday access.

If you have any questions, please contact me at (704) 758 3532 or erica.irvin@lowes.com.

Regards,

Erica M. Irvin
SVP, Commercial and Innovation Law

1000 Lowes Blvd.
Mooresville, NC 28117

October 9, 2024

[Full Name]
[Address 1]
[Address 2]
[City], [State] [Zip]

Notice of [Incident/Breach]

Dear [First Name]:

We are writing to let you know of a recent cybersecurity incident that affected some of your personal information.

We are providing you with information about the incident, our response, and additional measures you can take to help protect yourself.

What Happened?

On September 2, 2024, Lowe's detected unauthorized third-party access to certain employee's online Workday accounts. Workday is a third-party provider that supports some of Lowe's HR applications. Upon detecting the unauthorized access, we promptly activated our incident response procedures and launched an investigation into the nature and scope of the incident. Our investigation revealed that the unauthorized third party obtained a limited number of employees' Workday login information and gained temporary access to those employees' Workday accounts. If you are receiving this letter, then your Workday account was affected by this incident.

What Information Was Involved?

On September 9, 2024, we determined that the unauthorized third party obtained your Workday username and password. This means that the unauthorized third party also had access to certain information held in your Workday account, including your name, address, date of birth, email address, phone number, and bank account number.

What We Are Doing.

We are providing you with 12 months of complimentary credit monitoring services. Details about this offer and instructions on how to activate these services are enclosed with this letter.

Additionally, we are taking steps to strengthen our Workday authentication protocols and help protect access to your account, such as by resetting Workday passwords and implementing PIN multi-factor authentication for Workday access.

What You Can Do.

We encourage you to remain vigilant by reviewing account statements and monitoring free credit reports regularly to ensure there is no unauthorized or explained activity. We also encourage you to enroll in the complimentary credit monitoring services that we are offering. Please review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains details about this offer and general guidance on what you can do to safeguard against possible future misuse of your information.

Additionally, if you have not already done so, we recommend implementing Lowe's PIN multi-factor authentication to your Workday account. For more information, please visit internal-onprem.carbon.lowes.com.

For More Information.

If you have additional questions, you may contact us at the Associate Care Center at 844-475-6937 (844-HRLOWES) between 8:00 a.m. to 8:00 p.m. (Eastern Standard Time) Monday through Friday.

Sincerely,

Lowe's Privacy Office

Steps You Can Take to Help Protect Personal Information

Enroll in Experian's Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by 5:59pm CT on 1/31/2025** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bplus
- Provide your **activation code**: [Activation Code]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by 01/31/2025. Be prepared to provide engagement number B132218 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]

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

- **Credit Monitoring:** Actively monitors Experian file 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 receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance[2]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

<u>Monitor Your Accounts</u>

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

---

[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.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For Massachusetts residents, under Massachusetts law, individuals 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.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately three Rhode Island residents that may be impacted by this event