GT GreenbergTraurig

Kevin M. Scott
Tel 312.456.1040
Fax 312.803.2784
kevin.scott@gtlaw.com

December 29, 2025

Attorney General John Formella
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of Data Security Incident

Dear Attorney General Formella:

We represent Urban One, Inc ("Urban One"), located at 1010 Wayne Avenue 14th Floor, Silver Spring, MD 20910, and are writing to notify your office of an incident that may affect the security of some personal information relating to 2 New Hampshire residents.

Beginning on February 13, 2025, an unauthorized third party gained access to Urban One's network through a sophisticated social engineering campaign, which led to the unauthorized exfiltration of company data, including employee personal information. Urban One became aware of the incident on March 15, 2025, and, following its response process, immediately notified law enforcement, launched an investigation with the assistance of external cybersecurity experts to minimize incident impact, determine the scope of the incident, and assess what data may have been involved. While an initial notification was made on April 18, 2025, Urban One continued its extensive forensic analysis and manual document review, involving a large number of documents resulting in the identification of New Hampshire residents.

The personal information includes current and former employees' names, home address(es), Social Security numbers, financial account information, health insurance and medical information, and driver licenses.

Urban One takes the security of all information in its systems very seriously, and it has already taken steps to prevent a recurrence. Among other actions, the company has increased monitoring, further improved security controls, and reinforced its systems. Additionally, Urban One is offering individuals 24 months of identity protection (credit monitoring and identity theft restoration) services from Experian.

On or about December 29, 2025, Urban One began mailing notifications to the remaining potentially affected individuals. An example of the notification is attached.

Should you have any questions regarding this notification or other aspects of the data security incident, please contact me for any additional information.

Best Regards,

Kevin Scott
Shareholder

URBAN ONE
1010 Wayne Ave, 14th Floor, Silver Spring, MD 20910 301-429-3200

Return Mail Processing
PO Box 999
Suwanee, GA 30024

37 1 10580 **********AUTO**ALL FOR AADC 450
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

December 29, 2025

[Extra1]

Dear Sample A. Sample:

We write to provide notice of a data security incident that impacted some of your personal information. We take your trust and the security of your personal information very seriously, and we sincerely regret having to share this news with you. This letter contains information about what happened, actions we have taken to prevent a recurrence, and steps you can take to protect your information.

What Happened?
Beginning on February 13, 2025, an unauthorized third party gained access to our network through a sophisticated social engineering campaign, which led to the unauthorized exfiltration of company data, including current and former employee personal information. We became aware of the incident on March 15, 2025, and, following our incident response process, immediately notified law enforcement and launched an investigation with the assistance of external cybersecurity experts to minimize incident impact, determine the scope of the incident, and assess what data may have been involved. An initial notification was made while the investigation was ongoing and on October 27, 2025, we confirmed that certain personally identifiable information related to employees was obtained by a third party. We then worked to find contact information for those affected, obtain credit monitoring and identity protection services at no cost, and provide notification.

What Information Was Involved?
The data involved your first and last name, [Extra2].

What We Are Doing
Urban One takes the security of all information in our systems very seriously, and we want to assure you that we have already taken steps to prevent a recurrence. Among other actions, we have increased monitoring, further improved security controls, and reinforced our systems. We are providing credit monitoring services through Experian for all three major credit bureaus (Experian, Equifax, and TransUnion) for a period of 24 months at no cost to you. Enrollment instructions are enclosed. Please note that the deadline to enroll is March 31, 2026. We encourage you to enroll as soon as possible for maximum protection.

What You Can Do
We recommend that you:

- Enroll in the free credit monitoring services according to the instructions enclosed (federal law limits a cardholder's liability in the event of credit card fraud).
- Request an IRS Identity Protection PIN that prevents someone else from filing a tax return using your Social Security number or individual taxpayer identification number.
- Monitor your financial accounts for suspicious activity.
- Consider placing a fraud alert or credit freeze with each of the credit bureaus.

- Change passwords for your financial accounts and email.
- Enable two-factor authentication on online accounts where available.

Please also review the additional page enclosed, which contains more information on important steps you can take to protect your personal information and how you can enroll in credit monitoring and identity protection services through Experian.

For More Information
If you would like to request any additional information about this incident, please contact Experian at **(833) 918-9644, Monday through Friday, 9 am - 9 pm Eastern (excluding major U.S. holidays)**. Protecting your information is important to us. We appreciate your patience and understanding. Be prepared to provide your engagement number [Engagement Number].

Sincerely,

Karen Wishart
Urban One

Experian IdentityWorks^{SM}

If you believe there was fraudulent use of your information 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 24 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, including three-bureau credit monitoring, as a complimentary 24-month membership. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by March 31, 2026** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your activation code: **ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(833) 918-9644** by March 31, 2026. Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

Additional Important Information

Monitoring: You should always remain vigilant for incidents of fraud and identity theft, especially during the next 12-24 months, by reviewing financial account statements and monitoring your credit reports for suspicious or unusual activity and immediately report any suspicious activity or incidents of identity theft. You have the right to obtain or file a police report. You can contact the Federal Trade Commission (FTC) for more information on preventing identity theft. We encourage you to report any incidents of identity theft to the FTC.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.identitytheft.gov

Credit Reports: You may obtain a copy of your credit report, for free, whether or not you suspect any unauthorized activity on your account, from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You have the right to place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. To place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be needed to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-866-478-0027

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
http://www.experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800

For residents of *Iowa* and *Oregon*: You are advised to report any suspected identity theft to law enforcement or to the state Attorney General and Federal Trade Commission.

For residents of *New Mexico:* You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:
You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the FTC about fraud alerts, security freezes, and steps you can take to prevent identity theft. There were 2 Rhode Island residents notified of this incident.

District of Columbia Attorney General
400 6th Street NW
Washington, DC 20001
1-202-442-9828
www.oag.dc.gov

Maryland Office of Attorney General
200 St. Paul Pl
Baltimore, MD 21202
1-888-743-0023
https://www.marylandattorneygeneral.gov/

New York Attorney General
120 Broadway, 3rd Fl
New York, NY 10271
1-800-771-7755
www.ag.ny.gov

North Carolina Attorney General
9001 Mail Service Ctr
Raleigh, NC 27699
1-877-566-7226
https://ncdoj.gov/

Rhode Island Attorney General
150 South Main St
Providence RI 02903
1-401-274-4400
www.riag.ri.gov