The Washington Post

Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>
Enrollment Deadline: February 12, 2026
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

November 12, 2025

Subject: Notice of Data <<Security Incident/Breach>>

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a data security incident the Washington Post ("the Post") recently experienced that resulted from an unknown vulnerability in certain software we utilize from our vendor, Oracle. Please read this letter carefully, as this incident may have impacted some of your information. This letter is to notify you of the incident, offer you complimentary identity protection services, and inform you about steps you can take to help protect your personal information.

What Happened. On October 27, 2025, the Post learned that some of your personal information was potentially affected by a data security incident involving a previously unknown vulnerability affecting certain software from Oracle. The Post was recently contacted by a bad actor who claimed to have gained access to our Oracle E-Business Suite applications. In response, we launched a thorough investigation of our Oracle application environment with the assistance of forensic experts to determine if the environment had been accessed without authorization. During our investigation, we learned that Oracle had identified a previously unknown and widespread vulnerability in its E-Business Suite software that permitted unauthorized actors to access many Oracle customers' E-Business Suite applications. Our investigation confirmed that we were impacted by this exploit, and we discovered that, between July 10, 2025, and August 22, 2025, certain data was accessed and acquired without authorization. We then conducted a prompt review of the impacted data in order to determine what information was potentially affected and identify contact information for affected individuals. Please note that this Oracle vulnerability was unknown prior to this incident, has impacted many Oracle customers, and is not specific to the Post.

What Information Was Involved. The data that may have been acquired without authorization included your name and Social Security Number or tax ID number.

What We Are Doing. As noted above, we conducted a thorough investigation with the help of forensic experts, and promptly secured our systems and Oracle application environment, including by applying patches as soon as Oracle made them available. Out of an abundance of caution, we are also providing you with information about steps that you can take to help protect your personal information and are offering you <<12/24>> months of complimentary identity protection services from IDX at no charge to you. These services help detect possible misuse of your information and provide you with identity protection support.

What You Can Do. You can follow the recommendations included with this letter to help protect your information. In addition, you can enroll in IDX's complimentary identity protection services by visiting https://app.idx.us/account-creation/protect or calling (833) 781-8313. When enrolling, please provide the following unique code: <<ENROLLMENT>>. Please note that you must be at least 18 years of age to enroll in these services. As always, we encourage you to be vigilant in identifying potential phishing emails.

For More Information. For more information about how you can protect your information, please review the resources on the following page. If you have questions regarding the incident, please call (833) 781-8313, Monday through Friday, 9:00am to 9:00pm Eastern Time, excluding holidays.

The security of your information is a top priority for the Post. We take your trust in us and this matter very seriously, and we regret any worry or inconvenience that this may cause you.
Sincerely,

The Washington Post
1301 K. St. NW
Washington, DC 20071

Additional Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/get-credit-report

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. For TransUnion: www.transunion.com/credit-freeze.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/ CPD
888-743-0023

Oregon Attorney General
1162 Court St. NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General
The Capitol
Albany, NY 12224
ag.ny.gov
800-771-7755

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

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

Rhode Island: The Post has notified 9,562 individuals of this incident.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.