OCIPA Notification: Breach of ODOT Data

June 16, 2023

This notice is to inform you of a data breach. If you have a current Oregon driver's license or ID card, you are affected by this breach and this notice is for you.

What happened?

On Thursday, June 1, 2023, the State of Oregon became aware of a vulnerability in a third-party software tool. The software tool is called MOVEit, and the vulnerability was disclosed by the company that owns the software, Progress. MOVEit is a tool used to transfer data files.

Upon learning of the problem, the Oregon Department of Transportation (ODOT) quickly activated its emergency response procedures. ODOT worked with state cybersecurity professionals to immediately secure affected systems. ODOT also took immediate steps to investigate what, if any, of its information was affected by the vulnerability.

Unfortunately, on Monday, June 12, it was confirmed that the actors behind the hack of MOVEit Transfer accessed ODOT's data. This data contains personal information for approximately 3.5 million Oregonians. Even though the ODOT data was encrypted, it is widely understood that the hackers were able to read the data because of the vulnerability in MOVEit.

On Thursday, June 15, ODOT notified the public about the MOVEit Transfer breach.

This notification tells you more about the personal information accessed by the hackers, and what you can do to protect your identity.

What information was involved?

This information included personal information related to current, credentialed holders of Oregon driver's licenses or identification cards. The information protected by OCIPA is the combination of your first name, your last name, and driver's license or identification card number. This is "personal information" as defined under the Oregon Consumer Information Protection Act (OCIPA), ORS 646A.600 et seq.

This information also included dates of birth, physical addresses, and the last four digits of Social Security numbers. This information did not include banking, credit card or any other financial information. Your entire Social Security number was not part of this data.

We are making you aware of the incident as required by OCIPA, and so that you can take steps to protect your identity.

What we are doing.

ODOT is working closely with state cybersecurity services and has engaged a third-party security specialist for forensic analysis. This is a developing, world-wide issue, and ODOT is coordinating with local and federal law enforcement, sharing information as it becomes available and acting upon advisories provided by them. We will continue to closely monitor our systems, as well as vendor and industry information sources with information related to this vulnerability and its after-effects.

Information security and keeping personal information of Oregonians safe is our priority. We constantly update our security protocols to stay current with industry best practices. We will continue to guard against future vulnerabilities.

How you can reach us.

If you have any questions or concerns, please call 503-945-5000 or email ASKODOT@odot.oregon.gov

What you can do.

There are immediate steps you can take to protect your information from identity theft. We recommend you actively monitor your account statements and credit reports. You are entitled to a free copy of your credit report once every 12 months from each of the three major credit reporting agencies, Experian, Equifax, and TransUnion.

To order a **free** report visit www.annualcreditreport.com, call toll free 1-877-322-8228, or contact the bureaus directly.

You may contact the three credit bureaus individually:

Equifax Fraud Reporting
1-800-525-6285
P.O. Box 740256
Atlanta, GA 30374
www.alerts.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

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

You can also place fraud alerts with the three credit bureaus. Placing a fraud alert at one of the three major credit bureaus notifies the other two to place the same alert on their files for you. A fraud alert tells creditors to take certain steps, including contacting you, before they open any new accounts in your name or change your existing accounts. Placing a fraud alert can protect you, but means it will probably take more time for you to open new credit accounts. There is no charge for this protective measure. An initial fraud alert will last for one year.

If you ever believe you are the victim of identity theft, you should immediately file a police report with your local police department. A police report is often required to dispute fraudulent charges. You can also report suspected incidents of identity theft to local law enforcement, the Oregon Attorney General, and the Federal Trade Commission (FTC). The Oregon Attorney General and the FTC have additional information on preventative measures on their websites. Their contact information is:

Oregon Attorney General
1-877-877-9392

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
www.doi.state.or.us/

Federal Trade Commission
1-877-ID-THEFT (877-438-4338)
600 Pennsylvania Avenue, NW
Washington, DC 20580
http://www.ftc.gov/bcp/edu/microsites/idtheft/

OCIPA Description

The Oregon Consumer Information Protection Act (OCIPA), ORS 646A.600 et seq, is Oregon's law that protects consumers and ensures safety and security of sensitive and personal information. When there is a breach of security under OCIPA, the law sets clear direction and expectations for notification of individuals whose personal information was disclosed in the breach.

In accordance with OCIPA, this notification is intended to provide information on how consumers can protect their identity and monitor against fraud in light of this data breach.