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>>

Notice of Data Breach

Dear <<Name 1>>,

The State of Maine is encouraging individuals to take steps to protect their personal information following a worldwide cybersecurity issue affecting a widely used file transfer tool named MOVEit.

This global incident affected a wide range of industries, including insurance, finance, education, health, and government. This letter provides important details about the incident and outlines measures you can take to help protect your personal information. Please read it closely.

What Happened?

On May 31, 2023, the State of Maine became aware of a software vulnerability in MOVEit, a third-party file transfer tool owned by Progress Software and used by thousands of entities worldwide to send and receive data. As it pertains to the State, the software vulnerability was exploited by a group of cybercriminals and allowed them to access and download files belonging to certain agencies in the State of Maine between May 28, 2023, and May 29, 2023.

Importantly, as it pertains to the State, this incident was specific and limited to Maine's MOVEit server and did not impact any other State network or system.

Since the onset of the incident, the cybercriminals involved claimed their primary targets were businesses, with a promise to erase data from certain entities, including governments. Despite their assertions that any data obtained from governments has been erased, the State is urging individuals to take steps to protect their personal information.

What Information Was Involved?

The State might hold information about you for several reasons: you could be a resident, an employee, or you might have received services from or interacted with one of our state agencies. Additionally, the State participates in data sharing agreements with other organizations to enhance the services we offer to our residents and the public.

The specific information affected by this incident depends on the individual and their association with the State of Maine. After reviewing our records, we have determined that your information, which may have been involved, includes your name and <<Breached Elements>>.

What Are We Doing?

Upon discovery of the incident, the State immediately initiated measures to secure its information. This included blocking internet access to and from the MOVEit server and implementing security measures recommended by Progress Software to patch the vulnerability. The State also engaged the services of outside legal counsel, engaged external cybersecurity experts to investigate the nature and scope of the incident, and conducted a comprehensive investigation to determine what information was involved.

What Can You Do?

The State encourages you to consider the following recommendations to protect your personal information:

1. **Review Your Accounts for Suspicious Activity.** We encourage you to remain vigilant by regularly reviewing your accounts and monitoring credit reports for suspicious activity.

2. **Order A Credit Report.** If you are a U.S. resident, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. Contact information for the nationwide credit reporting agencies is provided in the next section.

3. **Contact the Federal Trade Commission, Law Enforcement, and Credit Bureaus**. You may contact the Federal Trade Commission ("FTC"), your state's Attorney General's office, or law enforcement, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's websites at www.identitytheft.gov and www.ftc.gov/idtheft; call the FTC at (877) IDTHEFT (438-4338); or write to: FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

   You may contact the nationwide reporting agencies at:

   a) Equifax: (800) 525-6285; P.O. Box 740241, Atlanta, Georgia, 30374; or www.equifax.com.

   b) Experian: (888) 397-3742; P.O. Box 9701, Allen, TX 75013; or www.experian.com.

   c) TransUnion: (800) 916-8800; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022; or www.transunion.com.

4. **Additional Rights Under the FCRA**. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You 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 you to review your rights pursuant to the Fair Credit Reporting Act by: (i) visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf; or (ii) by writing to Consumer Financial Protection Bureau, 1700 G Street, N.W., Washington, DC 20552.

5. **Request Fraud Alerts and Security Freezes**. You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

   To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	**Experian**	**TransUnion LLC**
P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (800) 525-6285	P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742	P.O. Box 6790 Fullerton, PA 92834-6790 https://www.transunion.com/fraud-alerts (800) 680-7289

   If you are concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/ 1-800-349-9960	P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze 1-888-397-3742	P.O. Box 2000 Chester, PA 19016 http://www.transunion.com/creditfreeze 1-888-909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

6. **For Iowa Residents**. You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

7. **For Maryland Residents**. You can obtain information about avoiding identity theft from the Maryland Attorney General at: Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023 (toll-free in Maryland), (410) 576-6300, www.marylandattorneygeneral.gov.

8. **For Massachusetts Residents**. You have the right to obtain a police report and request a security freeze (without any charge) as described above.

9. **For New York Residents**. You can obtain information about security breach response, identity theft prevention, and identity protection information from the New York State Office of the Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755 (toll-free), 1-800-788-9898 (TDD/TTY toll-free line), https://ag.ny.gov/, and at: Bureau of Internet and Technology (BIT), 28 Liberty Street, New York, NY 10005, Phone: (212) 416-8433, https://ag.ny.gov/resources/individuals/credit-lending/identity-theft.

10. **For North Carolina Residents**. You can obtain information about avoiding identity theft from the North Carolina Attorney General at: North Carolina Attorney General's Office 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free in North Carolina), (919) 716-6400, www.ncdoj.gov.

11. **For Residents of Oregon**. You may report suspected identity theft to law enforcement, including the Office of the Oregon Attorney General and the FTC. Contact information for the FTC is included in your notice. The Office of the Oregon Attorney General can be reached: (1) by mail at 1162 Court St. NE, Salem, OR 97301; (2) by phone at (877) 877-9392; or (3) online at https://www.doj.state.or.us/.

12. **For Rhode Island Residents**. You can obtain information about avoiding identity theft from the Rhode Island Office of the Attorney General at: Rhode Island Office of the Attorney General, Consumer Protection Unit 150, South Main Street, Providence, RI 02903, (401)-274-4400, www.riag.ri.gov. You have the right to obtain a police report, and to request a security freeze (charges may apply), as described above. Information pertaining to approximately 4 Rhode Island residents was potentially involved in this incident.

13. **For Washington, D.C. Residents**. You can obtain information about avoiding identity theft from the Office of the Attorney General for the District of Columbia at: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202)-727-3400, www.oag.dc.gov. You have the right to request a security freeze (without any charge) as described above.

Other Important Information.

The State has established a dedicated call center for individuals to call if they have any questions or concerns relating to the incident. The phone number is (877) 618-3659 and representatives are available Monday through Friday, 9 AM to 9 PM Eastern Time. Individuals can also visit www.maine.gov/moveit-global-data-security-incident for the latest information concerning this incident.

Sincerely,

The State of Maine