



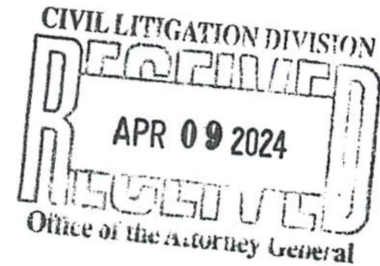
UNIVERSITY SYSTEM OF GEORGIA

270 Washington Street, S.W.
Atlanta, Georgia 30334

Phone: (404) 962-3000
Fax: (404) 962-3013

March 29, 2024

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202



Re: Data Breach Notice

Dear Sir or Madam:

Please accept this letter as the notice required by state law to inform your office of a data breach that impacted citizens of your state.

The Board of Regents of the University System of Georgia ("USG") purchased MOVEit® Secure File Transfer software from Progress® Software to transfer and store sensitive data. As has now been widely reported, the MOVEit® software included a vulnerability that allowed cybercriminals unauthorized access to the files stored on the MOVEit® platform at numerous government, higher education, and corporate customer sites worldwide beginning on or about May 28, 2023. This included USG. The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) have determined that data was acquired from the MOVEit® platform by a cybercriminal group named CL0P. The files and information obtained by this cybercriminal group will likely be published on its website. USG takes the protection of personal information seriously and is taking steps to prevent a similar occurrence in the future. MOVEit® Transfer software operating at USG was immediately blocked upon detection of the breach on May 31, 2023, and has now been fully updated and secured in accordance with guidance from Progress® Software and CISA.

A copy of the notice that USG intends to supply to citizens of your state is enclosed. This notification will be sent via U.S. Mail to the individual's last known address approximately one week after the date of this letter. USG has also supplied notification of this incident to the major consumer reporting agencies in the United States, and at least 12 months and up to 24 months of identity theft protection services have been offered to all individuals depending on state law requirements. Approximately 1500 citizens of Maryland were impacted by this breach.

Should you have any questions or need additional information, please send an email to: breachnotification@usg.edu.

Sincerely,

Alfred S. Barker
Chief Information Security Officer

Notice of Data Breach

Dear [FirstName] [LastName]:

The University System of Georgia (USG) was involved in an incident that may affect the security of your personal information. We want to provide you with information about the incident, steps we are taking in response, and steps you may take to guard against identity theft and fraud, should you feel it is appropriate to do so.

What Happened? USG purchased MOVEit® Secure File Transfer software from Progress® Software to transfer and store sensitive data. As has now been widely reported, the MOVEit® software included a vulnerability that allowed cybercriminals unauthorized access to the files stored on the MOVEit® platform at numerous government, higher education, and corporate customer sites worldwide beginning on or about May 28, 2023. This included USG. The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) have determined that data was acquired from the MOVEit® platform by a cybercriminal group named CL0P. The files and information obtained by this cybercriminal group will likely be published on its website.

What Information Was Involved? Data related to you may include:

- Full or partial (last 4 digits) Social Security Number
- Date of Birth
- Bank account number(s)
- Federal income tax documents with Tax ID number

What We Are Doing. USG takes protecting your personal information seriously and is taking steps to prevent a similar occurrence in the future. MOVEit® Transfer software operating at USG was immediately blocked upon detection of the breach on May 31, 2023, and has now been fully updated and secured in accordance with guidance from Progress® Software and CISA. After updating and securing the system, USG immediately began a lengthy investigation to determine which individuals may have been impacted by the incident.

What You Can Do. You can review information from the Federal Trade Commission's website, <https://IdentityTheft.gov/databreach>, for steps to help protect yourself from identity theft. In addition, we recommend you take advantage of free credit monitoring and related services offered to you via Experian using the instructions below.

Other Important Information:

To help protect your identity, USG is offering complimentary access to Experian IdentityWorksSM for [TERM] months.

If you believe there was fraudulent use of your information because 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. This includes investigating and resolving 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 [TERM] 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 [TERM]-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 July 31, 2024** (Your code will not work after this date.).
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: **[Activation Code]**

If you have questions about the product, need assistance with Identity Restoration that arose because of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team toll-free at **833-918-1243** by July 31, 2024. Be prepared to provide engagement number **[ENGAGEMENT]** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [TERM]-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*.
- **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**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information. USG regrets any inconvenience or concern caused by this incident. If you have further questions or concerns or would like an alternative to enrolling online, please call **833-918-1243** toll-free Monday through Friday from 8 a.m. – to 10 p.m. Central or Saturday and Sunday from 10 a.m. – 7 p.m. Central (excluding major U.S. holidays). Be prepared to provide your engagement number **[ENGAGEMENT]**.

USG encourages you to remain vigilant and review your personal account statements and monitor free credit reports. You may also contact the major consumer reporting agencies to request a security freeze free of charge as provided by federal law. To obtain a credit freeze, you will generally need to provide your Social Security Number, date of birth, and address. The contact information for the major consumer reporting agencies is:

- Equifax: PO Box 740241, Atlanta, GA 30347 1-800-525-6285 ([equifax.com](https://www.equifax.com))
- Experian: PO Box 9554, Allen, TX 75013, 1-888-397-3742 ([experian.com](https://www.experian.com))
- TransUnion: PO Box 2000, Chester, PA 19016, 1-800-680-7289 ([transunion.com](https://www.transunion.com))

For additional information regarding steps to take to avoid identity theft including fraud alerts and security freezes, you may also contact the Federal Trade Commission at 600 Pennsylvania Ave., NW, Washington, DC 20580, (202) 326-2222 or 1-877-FTC-HELP and see [identitytheft.gov](https://www.identitytheft.gov) and <https://www.identitytheft.gov/#/Know-Your-Rights>. All United States citizens have additional rights pursuant to the U.S. Fair Credit Reporting Act. Residents of the District of Columbia may also contact the Office of the Attorney General for the District of Columbia. Iowa residents should report suspected identity theft to local law enforcement or the Iowa Attorney General. Maryland residents may also contact the Maryland Attorney General for additional information at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; or at www.marylandattorneygeneral.gov. A Massachusetts resident has the right to obtain a police report. New York residents may obtain additional information from the New York State Attorney General's website: ag.ny.gov/resources/credit-lending/identity-theft. North Carolina residents may obtain additional information from the North Carolina Attorney General's office at 9001 Mail Service Center, Raleigh, NC, 27699-9001, 919-716-6400, ncdoj.gov. Rhode Island residents may obtain a police report and may also obtain additional information from the Rhode Island Attorney General at www.riag.ri.gov (401) 274-4400. You should report suspected identity theft to law enforcement, including to your state's attorney general and to the Federal Trade Commission.

Sincerely,

Alfred S. Barker, Chief Information Security Officer
University System of Georgia
270 Washington St., SW

Atlanta, GA 30334

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** 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 at <https://www.experianidworks.com/summary-of-benefits-june-2019>. Coverage may not be available in all jurisdictions.

BOARD OF REGENTS OF THE UNIVERSITY SYSTEM OF GEORGIA

270 WASHINGTON STREET, S.W.

ATLANTA, GEORGIA 30334

Presort
First Class Mail
ComBasPrice



US POSTAGE PAID PITNEY BOWES



ZIP 30334 \$ 000.54⁷
02 4W
0000358407 APR 01 2024

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

14

CEGOAAB

21202

