



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Angelina W. Freind
Office: (267) 930-4782
Fax: (267) 930-4771
Email: afreind@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

November 3, 2023

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Westat, Inc. ("Westat") located at 1600 Research Boulevard, Rockville, Maryland 20850. Westat is writing to notify your Office of an incident that may affect the privacy of certain personal information relating to approximately thirty-eight (38) Maryland residents. Westat provides research support and services pursuant to contracts with certain governmental agencies with whom it worked to provide notification to data owners participating in certain studies. As a result of this event, Westat is issuing notification to impacted individuals on behalf and with the permission of certain data owners, including Berkeley Medical Center. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Westat does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

Westat utilized MOVEit Transfer ("MOVEit") third-party software to manage data it collected and/or maintained on behalf of other organizations. On May 30, 2023, Westat detected unusual activity occurring in its MOVEit instance and later that day MOVEit announced a zero-day vulnerability that had impacted a large number of companies across various industries. Westat immediately took steps to ensure the security of its environment, and with the assistance of third-party forensic specialists, conducted an investigation to determine the nature and scope of the activity.

The investigation determined that certain data stored on the MOVEit server may have been copied without authorization between May 28 and May 29, 2023. Westat conducted a detailed review of data involved to determine the type of information that was present and to whom it related. This review confirmed that certain information belonging to data owners was present in the impacted data, and was accessed or acquired during the MOVEit incident. Upon completion of this analysis, Westat notified governmental agency partners and impacted data owners and is now providing notification to impacted individuals at the direction of impacted data owners.

The personal information related to Maryland residents that could have been copied by the unauthorized actor includes name, medical record number/identifier, date of birth, date and/or time of service, zip code, and condition or disposition.

Notice to Maryland Residents

On November 3, 2023, Westat began providing written notice of this event to affected individuals on behalf of certain data owners. Approximately thirty-eight (38) Maryland residents are associated with Berkeley Medical Center. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Notification is also being provided pursuant to the Health Insurance Portability and Accountability Act (“HIPAA”).

Other Steps Taken and To Be Taken

Upon becoming aware of the event, Westat moved quickly to investigate and respond to the incident, assess the security of Westat systems, identify potentially affected individuals, and notify governmental agency partners and data owners. Further, Westat notified federal law enforcement regarding the event. Westat is also working to implement additional safeguards and training to its employees. Westat is providing access to credit monitoring services through IDX, to certain individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Westat is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to the associated institutions. Westat is providing individuals with information on how to place a fraud alert and credit freeze on one’s credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Westat is providing written notice of this incident to relevant state and federal regulators, as necessary. Westat is also notifying the U.S. Department of Health and Human Services and prominent media pursuant to HIPAA.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4782.

Very truly yours,

Angelina W. Freind of
MULLEN COUGHLIN LLC

AWF/aml
Enclosure

EXHIBIT A



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

Enrollment Code: <<Enrollment Code>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

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

November 3, 2023

NOTICE OF DATA INCIDENT

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

Westat, Inc. ("Westat" or "We") conducts data collection and related activities in support of the Drug Abuse Warning Network ("DAWN"). DAWN is a public health surveillance system that collects data on drug-related emergency department visits (<https://www.samhsa.gov/data/data-we-collect/dawn-drug-abuse-warning-network>). <<Covered Entity>> participates in and provides certain patient information to DAWN for the purpose of capturing data related to emergency department visits related to substance use and misuse. We are writing to make you aware of a data incident that may impact the privacy of your personal information.

What Happened? Westat uses a tool called MOVEit Transfer ("MOVEit") to manage DAWN data. MOVEit recently discovered a flaw within the tool. On May 30, 2023, Westat learned that the MOVEit flaw impacted our systems. We took steps to shut down the MOVEit tool. We also began an investigation to understand what DAWN data was exposed.

We learned that your data was copied or taken without permission. This happened between May 28 and May 29, 2023. After learning this, Westat reported this discovery to <<Covered Entity>> from whom it received your information and is now providing notification on that entity's behalf.

What Information Was Involved? Your name, <<Data Elements>> were present in the impacted files. Although these data elements were present in the impacted files, your medical record with the hospital was not exposed as a result of this incident. We have no evidence that any of your information was used for identity theft or fraud.

What We Are Doing? We take this incident and the obligation to safeguard the information in our care very seriously. After discovering the incident, we promptly took steps to confirm our system security, and engaged with a third-party forensic specialist to assist in conducting a comprehensive investigation. Further, we have implemented all software security patches provided by MOVEit to date. As an added precaution, we are offering 12 months of credit monitoring and identity restoration services through IDX, a ZeroFox Company. If you wish to activate these complimentary services, you may follow the instructions included in the attached *Steps You Can Take to Help Protect Your Personal Information*. We encourage you to enroll in these services as we are unable to act on your behalf to do so.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months.

For More Information. If you have additional questions or concerns, please feel free to call us at 1-888-566-8328. We are available Monday through Friday 9 am – 9 pm Eastern Time. You may also write to Westat at Westat, Inc., RB 4124, 1600 Research Blvd, Rockville, MD 20850.

Sincerely,

A handwritten signature in black ink that reads "Dennis Pickett". The script is cursive and fluid, with the first letters of "Dennis" and "Pickett" being capitalized and prominent.

Dennis Pickett
Vice President
Chief Information Security Officer
Westat

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring and Identity Restoration Services

1. Website and Enrollment. Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you. Please note the deadline to enroll is February 3, 2024.

3. Telephone. Contact IDX at 1-888-566-8328 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported promptly to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 2 Rhode Island residents that may be impacted by this event.