

July 28, 2023

VIA EMAIL

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

Re: Notice of Data Security Incident

To Whom It May Concern:

I am providing the following notice of a security incident on behalf of our client, Allegheny County, Pennsylvania (the "County"). This incident impacted 144 Maryland residents.

Notice of the incident will be provided via website notice and media notice on or about July 28, 2023. The County will also be providing notice of the incident via U.S. mail to those individuals who the County has sufficient contact information for.

What Happened

On June 1, 2023, the County became aware of a software vulnerability in MOVEit, which is a popular file transfer tool owned by Progress Software and used by the County to send and receive data. This vulnerability was exploited by a group of cybercriminals known as "CI0p," and allowed them to access and download files between May 28, 2023, and May 29, 2023.

Since the onset of the incident, CI0p has maintained that it is focused on targeting businesses and that it will delete any data from certain organizations, including governments. While CI0p indicated that it has deleted data specifically belonging to Allegheny County, the County is still encouraging individuals to take precautionary steps to protect their personal information.

What Information Was Involved

While the impacted information varies based on the individual at issue and their relationship with Allegheny County, this incident involved the following information: name; Social Security number (SSN); date of birth; driver's license/state identification number; taxpayer identification number; and student identification numbers. For some individuals, certain types of medical information

(e.g., diagnosis, treatment type, admission date), health insurance information, and billing/claim information may be involved.

Remedial Steps

As soon as the County became aware of the incident, it took steps to secure its information, including blocking access to and from the MOVEit server and implementing security measures recommended by Progress Software to patch the vulnerability. The County also engaged external cybersecurity experts to investigate the nature and scope of the incident and conducted an extensive investigation to determine what information was involved. The County is also partnering with IDX to offer 24 months of complimentary credit monitoring to affected individuals whose Social Security numbers were involved in this incident.

Should you have any questions or concerns about this matter, please do not hesitate to contact me using the information provided below.

Sincerely,



Sadia Mirza
Direct: 949.622.2786
Email: sadia.mirza@troutman.com

Logo/Allegheny County

<<Return Address>>
<<City>>, <<State>> <<Zip>>

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

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

<<Date>>

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

Allegheny County is encouraging individuals to take precautionary action to protect their personal information in the wake of a global cybersecurity incident impacting a popular file transfer tool called MOVEit. Like hundreds of businesses from various industries – including insurance, finance, government, and health care, Allegheny County was affected by the incident. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened?

On June 1, 2023, the County became aware of a software vulnerability in MOVEit, which is a popular file transfer tool owned by Progress Software and used by the County to send and receive data. This vulnerability was exploited by a group of cybercriminals known as “Cl0p,” and allowed them to access and download files belonging to the County between May 28, 2023 - May 29, 2023.

Since the onset of the incident, Cl0p has maintained that it is focused on targeting businesses and that it will delete any data from certain organizations, including governments. While Cl0p indicated that it has deleted data specifically belonging to Allegheny County, the County is still encouraging individuals to take precautionary steps to protect their personal information.

What Information Was Involved?

While the impacted information varies based on the individual at issue and their relationship with Allegheny County, we reviewed our records and determined the following information of yours may have been involved: Name and <<Variable Data>>.

What Are We Doing?

As soon as the County became aware of the incident, the County took steps to secure its information, including by blocking access to and from the MOVEit server, and implemented security measures recommended by Progress Software to patch

the vulnerability. The County also engaged external cybersecurity experts to investigate the nature and scope of the incident, and conducted an extensive investigation to determine what information was involved. Law enforcement was also notified.

The County is now partnering with IDX to offer 24 months of complimentary credit monitoring to affected individuals whose Social Security numbers were involved in this incident. A description of the benefits and enrollment instructions for the complimentary credit monitoring services is provided below.

What Can You Do?

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

1. Register for Identity Protection Services. We have arranged for IDX to provide individuals whose SSNs were involved in this incident with two years of complimentary identity protection services. These services provide access to the following:
 - **Single Bureau Credit Monitoring (for adults).** Monitoring of credit bureau for changes to your credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in your credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities.
 - **CyberScan.** Dark web monitoring of underground websites, chat rooms, and malware to identify trading or selling of personal information.
 - **Identity Theft Insurance.** Identity theft insurance will reimburse you for expenses associated with restoring your identity should you become a victim of identity theft. If your identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best “A-rated” carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.
 - **Managed Identity Recovery Service.** This service provides restoration for identity theft issues such as: account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation.

We encourage you to contact IDX with any questions including with respect to the complimentary identity protection services by calling (888) 990-1333. IDX representatives are available Monday through Friday from 9 AM to 9 PM Eastern Time.

In order to receive the complimentary identity protection services described above, individuals must enroll by Enrollment Deadline.

2. Review Your Accounts for Suspicious Activity. We encourage you to remain vigilant by regularly reviewing your accounts and monitoring credit reports for suspicious activity.
3. 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.
4. 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 credit 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.

5. **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/bcfc_consumer-rights-summary_2018-09.pdf; or (ii) by writing to Consumer Financial Protection Bureau, 1700 G Street, N.W., Washington, DC 20552.

6. **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.

In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze at no cost to you:

- a) Equifax: (800) 349-9960
- b) Experian: (888) 397-3742
- c) TransUnion: (888) 909-8872

Placing a security freeze prohibits the agency from releasing any information about your credit report without your written authorization. Security freezes must be placed separately at each of the three nationwide credit reporting agencies. When requesting a security freeze, you may need to provide the following information:

- Your full name, with middle initial as well as Jr., Sr., II, etc.
- Social Security number
- Date of birth
- Current address and all addresses for the past two years
- Proof of current address, such as a current utility bill or telephone bill
- Legible copy of a government-issued identification card, such as a state driver’s license, state identification card, or military identification.

After receiving your request, each agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

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 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/internet/resource-center>.
9. 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.
10. 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/>.
11. 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.
12. 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 County 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 (888) 990-1333 and representatives are available Monday through Friday, 9 AM to 9 PM Eastern Time.

Sincerely,

Allegheny County

Logo/Allegheny County

<<Return Address>>
<<City>>, <<State>> <<Zip>>

To the Parent or Guardian of
<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Notice of Data Breach

Dear Parent or Guardian of <<First Name>> <<Last Name>>,

Allegheny County is encouraging individuals to take precautionary action to protect their personal information in the wake of a global cybersecurity incident impacting a popular file transfer tool called MOVEit. Like hundreds of businesses from various industries – including insurance, finance, government, and health care, Allegheny County was affected by the incident. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your child’s personal information.

What Happened?

On June 1, 2023, the County became aware of a software vulnerability in MOVEit, which is a popular file transfer tool owned by Progress Software and used by the County to send and receive data. This vulnerability was exploited by a group of cybercriminals known as “Cl0p,” and allowed them to access and download files belonging to the County between May 28, 2023 - May 29, 2023.

Since the onset of the incident, Cl0p has maintained that it is focused on targeting businesses and that it will delete any data from certain organizations, including governments. While Cl0p indicated that it has deleted data specifically belonging to Allegheny County, the County is still encouraging individuals to take precautionary steps to protect their personal information.

What Information Was Involved?

While the impacted information varies based on the individual at issue and their relationship with Allegheny County, we reviewed our records and determined the following information of your child may have been involved: Name and <<Variable Data>>.

What Are We Doing?

As soon as the County became aware of the incident, the County took steps to secure its information, including by blocking access to and from the MOVEit server, and implemented security measures recommended by Progress Software to patch the vulnerability. The County also engaged external cybersecurity experts to investigate the nature and scope of the incident, and conducted an extensive investigation to determine what information was involved. Law enforcement was also notified.

What Can You Do?

The County 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 credit 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.

In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze at no cost to you:

- a) Equifax: (800) 349-9960
- b) Experian: (888) 397-3742
- c) TransUnion: (888) 909-8872

Placing a security freeze prohibits the agency from releasing any information about your credit report without your written authorization. Security freezes must be placed separately at each of the three nationwide credit reporting agencies. When requesting a security freeze, you may need to provide the following information:

- Your full name, with middle initial as well as Jr., Sr., II, etc.
- Social Security number
- Date of birth
- Current address and all addresses for the past two years
- Proof of current address, such as a current utility bill or telephone bill
- Legible copy of a government-issued identification card, such as a state driver's license, state identification card, or military identification.

After receiving your request, each agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

6. 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.
7. 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/internet/resource-center>.
8. 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.
9. 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/>.
10. 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.
11. 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 County 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 (888) 990-1333 and representatives are available Monday through Friday, 9 AM to 9 PM Eastern Time.

Sincerely,

Allegheny County