

July 10, 2023

Jeff Karberg, Administrator of the
Identity Theft Program
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Dear Mr. Karberg:

In accordance with the Maryland Personal Information Protection Act, please accept this letter as the Tidewater Youth Services Commission's notice to the Office of the Attorney General, in accordance with Maryland Commercial Law Code § 14-3504.

On or about February 12, 2023, the Tidewater Youth Services Commission (the "Commission") became aware that it was the victim of a ransomware attack. Immediately the Commission's leadership, IT, third-party experts, and law enforcement were engaged to mitigate the effects of the attack, secure personal information, and protect the Commission's network from additional compromise.

To date, our investigation revealed that sometime before February 12, 2023, threat actors gained access to the Commission's network environment likely through a phishing campaign. The threat actors then enumerated and encrypted the network. The investigation cannot confirm if personal information was exfiltrated from the network. Therefore, approximately 2 Maryland residents may have potentially been affected by this data incident. To date, there is no evidence that personal information from any potentially affected individual has been misused.

Out of an abundance of caution and in accordance with Maryland law, the Commission is notifying those potentially affected. The notices to those potentially affected will contain information about the incident, how to protect themselves, and how to obtain free credit reports. The draft notice letter is enclosed herein.

Notice to the Attorney General was delayed due to the Commission's efforts to identify affected individuals from systems that were identified as compromised.

For further information about this data incident, you may contact Darius Davenport, at ddavenport@cwm-law.com.

Sincerely,

Jenny Hodge, U.S.N., M.D.

Jenny Hodge
Executive Director

July 10, 2023

Dear _____:

Tidewater Youth Services Commission (the "Commission") writes to notify you of a data security incident that may have impacted you. This letter is to inform you about the incident, our response, and steps you may take to protect against possible misuse of your personal information, should you feel it appropriate to do so.

What Happened? On or about February 12, 2023, the Commission became aware that it was the victim of a ransomware attack. The Commission's management, IT, and third-party information technology experts were engaged to investigate the incident, secure personal information and protect the Commission's network from additional compromise. Our investigation revealed that malicious actors gained access to the network on or about February 12, 2023, and deployed ransomware to encrypt the network. There is no definitive evidence that your personal information was accessed. However, because an unknown actor gained access to our network, we are providing this notice out of an abundance of caution. To date, we have not received any indication that your information has been misused by an unauthorized individual.

What Information Was Involved? It is possible that your Social Security number, military ID number, date of birth, passport number and financial account information may have been seen or accessed. This information is called your personal information. It tells others about you and is a part of your identity.

What We Are Doing. We take the confidentiality, privacy, and security of information in our care seriously. Information technology experts were immediately engaged and commenced an investigation to determine the nature and scope of the incident. While investigation remains ongoing, we are taking steps now to implement additional safeguards and review policies and procedures relating to data privacy and security.

The Commission has implemented additional security measures designed to prevent a reoccurrence of such incidents, and to protect the privacy of our employees, students and vendors. Among other steps taken, we have installed a more robust cloud-based cybersecurity solution across our network, strengthened our system's architecture, and implemented stronger policies to prevent future attacks.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. We also encourage you to review the "Steps You Can Take to Help Protect Your Information" pages enclosed herein.

For More Information. We understand that you may have some questions about this incident that are not addressed in this letter. Should you have additional questions, please contact Altreese Allmond at (757) 335-0290 9:00 a.m. to 5:00 p.m. Eastern Standard Time, Monday through Friday excluding major US holidays.

We apologize for any inconvenience that may have arose as a result of this incident. In the meantime, we ask for your understanding and patience.

Sincerely,

Jenny Hodge, M.P.H., M.D.

Jenny Hodge
Executive Director

Steps You Can Take to Help Protect Your Information

Check Your Accounts

We urge you to stay alert for incidents of identity theft and fraud, review your account statements, and check your credit reports for suspicious activity. Under U.S. law, you are eligible for one free credit report each year from each of the three major credit reporting bureaus. To order your free credit report, visit annualcreditreport.com or call toll-free 877-322-8228. You may also reach out to the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a security freeze on your credit report. The security freeze will stop a consumer reporting agency from giving out personal or financial information in your credit report without your consent. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. Note: using a security freeze to take control over who gets access to your credit report may delay or prevent any new loan, credit, mortgage, or any other credit extension request or application you make from being approved timely. Under federal law, you cannot be charged to place or lift a security freeze on your credit report. If you wish to place a security freeze, please reach out to these major consumer reporting agencies:

Experian

P.O. Box 9554
Allen, TX 75013
888-397-3742

experian.com/freeze/center

TransUnion

P.O. Box 160
Woodlyn, PA 19094
888-909-8872

transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
800-685-1111

quifax.com/personal/credit-report-services

To request a security freeze, you will need to provide these items:

1. Your full name with middle initial and suffix (Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. The addresses where you have lived over the last five years, if you have moved
5. Proof of current address, such as a current utility bill or telephone bill
6. A clear photocopy of a government-issued identification card (state driver's license or ID card, military ID, etc.)
7. If you are a victim of identity theft, show a copy of either the police or investigative report or complaint to a law enforcement agency about identity theft

Instead of a security freeze, you have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Businesses are required to take steps to verify a consumer's identity before extending new credit once they see a fraud alert on a credit file. If you are a victim of identity theft, you are eligible for an extended fraud alert. This is a fraud alert lasting seven years. If you wish to place a fraud alert, please reach out to any one of these agencies:

Experian
P.O. Box 9554
Allen, TX 75013
888-397-3742
experian.com/fraud

TransUnion
P.O. Box 2000
Chester, PA 19016
800-680-7289
transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
888-766-0008
equifax.com/personal/credit-report-services

More Information

You can learn more about identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by reaching out to:

- The consumer reporting agencies.
- The Federal Trade Commission at: 600 Pennsylvania Ave. NW, Washington, DC 20580, identitytheft.gov, 877-ID-THEFT (877-438-4338); TTY: 866-653-4261.
 - The FTC also urges those who learn their information has been misused to file a complaint with them. Reach out to the FTC for steps to file such a complaint.
- Your state Attorney General.

You have the right to file a police report if identity theft or fraud ever happen to you. Note: to file a report with law enforcement for identity theft, you will need to give some proof you have been a victim. Also, you must report cases of known or presumed identity theft to law enforcement and your state Attorney General.

All U.S. Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580, consumer.gov/idtheft, 877-IDTHEFT (877-438-4338), TTY: 866-653-4261.

California Residents: Visit the California Office of Privacy Protection (oag.ca.gov/privacy) for more information to protect yourself against identity theft.

Florida Residents: Office of the Attorney General of Florida, 1-866-966-7226 (Fraud Hotline), <http://myfloridalegal.com/identitytheft>.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Ave., Ste. 118, Frankfort, KY 40601, ag.ky.gov, 502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, 888-743-0023 or 410-528-8662.

New Mexico Residents: You have rights under the Fair Credit Reporting Act, such as the rights to:

- Be told if information in your credit file has been used against you.
- Know what is in your credit file.
- Ask for your credit score.
- Dispute lacking or wrong information.

Also, under the Fair Credit Reporting Act:

- The consumer reporting agencies must correct or delete wrong, lacking, or unverifiable information.
- The consumer reporting agencies may not report outdated bad information.
- Access to your file is limited.
- You must give your consent for credit reports to be given to employers.
- You may limit “prescreened” credit and insurance offers you get based on information in your credit report.
- You may seek damages from a violator.

You may have more rights under the Act not reviewed here. Identity theft victims and active duty military personnel have more specific rights under the Act. You can review your rights under the Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing to: Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

New York Residents: Contact the Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 800-771-7755; <https://ag.ny.gov>.

North Carolina Residents: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 919-716-6400, 877-566-7226 (toll free within NC).

Oregon Residents: Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, www.doj.state.or.us, 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 S. Main St., Providence, RI 02903, www.riag.ri.gov, 401-274-4400. Under Rhode Island law, you have the right to get any police report filed about this incident.

Washington D.C. Residents: Reach the Office of Attorney General for the District of Columbia at: 400 6th St. NW, Washington, DC 20001; 202-442-9828; <https://oag.dc.gov>.