MARSHALL DENNEHEY
WARNER COLEMAN & GOGGIN
ATTORNEYS-AT-LAW WWW.MARSHALLDENNEHEY.COM
A PROFESSIONAL CORPORATION
2000 Market Street, Suite 2300 · Philadelphia, PA 19103
(215) 575-2600 · Fax (215) 575-0856

PENNSYLVANIA
Allentown
Doylestown
Erie
Harrisburg
King of Prussia
Philadelphia
Pittsburgh
Scranton
NEW JERSEY
Cherry Hill
Roseland
DELAWARE
Wilmington
OHIO
Cincinnati
Cleveland
FLORIDA
Ft. Lauderdale
Jacksonville
Orlando
Tampa
NEW YORK
Long Island
New York City
Westchester

Direct Dial: 215-575-2615
Email: djshannon@mdwcg.com

August 9, 2017

Via Email: attorneygeneral@doj.nh.gov
Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Wooster-Ashland Regional Council of Governments
Our File No. 04949.00121

Dear Attorney General Foster:

Pursuant to N.H. Rev. Stat. Ann. § 359-C:20(I)(b), we are writing to notify you of a data security incident involving 22 New Hampshire residents. We are submitting this notification on behalf of our client, Wooster-Ashland Regional Council of Governments ("WARCOG").

Nature Of The Security Breach

WARCOG is a governmental entity located in the City of Wooster, Ohio. On or about June 28, 2017, the FBI notified WARCOG that WARCOG was the victim of a cyber attack by which an unknown third-party was able to access a computer file containing the personal information of individuals listed within police incident reports originating in the Cities of Wooster, Ashland, and Orrville over the last ten years. As a result, some of the personal information belonging to New Hampshire residents who were involved in an incident involving the police in one of these cities in the last ten years may have been exposed to others, including their first and last names, home addresses, dates of birth, social security numbers, and driver's license numbers.

The residents involved in this incident were forwarded letters notifying them of this incident on August 7, 2017. A copy of the form letter is attached hereto.

Steps Taken Relating To The Incident

Upon learning of the cyber-attack, WARCOG took steps to address this incident promptly after it was discovered, including undertaking an internal investigation of the matter in order to develop a better understanding of what had taken place and how. The FBI is currently investigating the incident. WARCOG also reported the incident to local law enforcement, which is also investigating. This notification was not

delayed as a result of a law enforcement investigation. WARCOG also engaged the services of an independent computer forensic firm to ensure that the computer system is more secure. WARCOG is in the process of reviewing its internal policies and data management protocols and has implemented enhanced security measures to help prevent this type of incident from recurring in the future.

WARCOG has also arranged to have Equifax protect the affected individuals' identity for one year at no cost to them through its Credit Watch ™ Silver credit monitoring and identity theft protection service. This service offers additional layers of protection including credit monitoring and a $25,000 identity theft insurance policy.

Should you need additional information regarding this matter, please contact me.

Very truly yours,

DS

DAVID J. SHANNON

DJS:jl
Encl.

WOOSTER-ASHLAND REGIONAL COUNCIL OF GOVERNMENTS

Wooster-Ashland
Regional Council of Governments
538 N. Market St.
Wooster, Oh 44691

Return Service Requested

City of Ashland
206 Claremont Ave.
Ashland, Ohio 44805

City of Orrville
207 N. Main St.
Orrville, OH 44667

City of Wooster
538 N. Market St.
Wooster, OH 44691

00162
JOHN DOE
123 ANYSTREET RD
STRAWBERRY AK 72469

NOTICE OF DATA BREACH

We are writing to notify you about a data breach that recently occurred involving the Wooster-Ashland Regional Council of Governments (WARCOG). This incident may have involved some of your personal information. As a result, your personal information may have been potentially exposed to others. The privacy and protection of your information are a matter that we take very seriously. Please be assured that we have taken every step necessary to address the incident and that we are committed to fully protecting all of the information that you have entrusted to us. Please review the information provided in this notice for some steps that you may take to protect yourself against any potential misuse of your information.

What Happened

On or about June 28, 2017, the FBI notified WARCOG that it was the victim of a cyber attack by which an unknown third-party was able to access a computer file containing the personal information of individuals listed within police incident reports originating in the Cities of Wooster, Ashland, and Orrville over the last ten years. As a result, if you were involved in an incident involving the police in one of these cities in the last ten years, some of your personal information may have been exposed to others.

What Information Was Involved

Based on our internal investigation of this matter, we have determined that the personal information potentially at risk of being accessed included first and last names, home addresses, dates of birth, social security numbers, and driver's license numbers.

What We Are Doing

Everything we can. We take the privacy and protection of our residents' personal information very seriously, and we deeply regret that this incident occurred. We took steps to address this incident promptly after it was discovered, including undertaking an internal investigation of the matter to develop a better understanding of what had taken place and how. The FBI is currently investigating the incident. We also reported the incident to local law enforcement, which is also investigating. This notification was not delayed as a result of a law enforcement investigation. We have also engaged the services of an independent computer forensic firm to

ensure that the computer system is more secure. We are in the process of reviewing our internal policies and data management protocols and have implemented enhanced security measures to help prevent this type of incident from recurring in the future.

Securing your personal information is important to us. As a precautionary measure to help better protect your credit file from potential misuse, we have partnered with Equifax ® to provide its Credit Watch ™ Silver credit monitoring and identity theft protection product for one year at no charge to you. A description of this product is provided in the attached material, which also contains instructions on how to enroll (including your personal activation code).

If you choose to take advantage of this product, it will provide you with a notification of key changes to your Equifax credit file, up to $25,000 Identity Theft Insurance Coverage, automatic fraud alerts, access to your Equifax credit report and Identity Restoration. If you become a victim of identity theft, an Equifax identity restoration specialist will work on your behalf to help you restore your identity.

Even if you decide not to take advantage of the subscription offer, you may still receive Equifax Identity Restoration in the event that you become a victim of identity theft by calling 877-368-4940, 9:00 a.m. to 8:00 p.m. Eastern, Monday through Friday, before **July 31, 2018**.

You must complete the enrollment process for Equifax Credit Watch™ Silver by **October 31, 2017**. We urge you to consider enrolling in this product, at our expense and reviewing the Additional Resources enclosed with this letter.

What You Can Do

You can take the following steps to guard against identity theft and fraud:

- Register for the complimentary credit monitoring services provided at no cost to you, as discussed in this notice.

- Review the enclosed "Information About Identity Theft Protection" reference guide, which describes additional steps that you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding your identity theft protection.

For More Information

If you have any questions about this incident or any of the products we are making available to you, you may call Epiq, the company through which these products are provided. Epiq's agents are available Monday through Friday from 9:00a.m. to 9:00p.m. EST at **1-800-930-0514**.
Once again, the privacy and protection of your information is a matter we take very seriously, and we sincerely apologize for any concern that this may cause you.

Sincerely,

Executive Committee of the Wooster-Ashland Regional Council of Governments

Bob Breneman	*David Handwerk*	*Duane Fishpaw*
Mayor Bob Breneman	Mayor David Handwerk	Mayor Duane Fishpaw
City of Wooster	City of Orrville	City of Ashland

EQUIFAX®

Activation Code:

About the Equifax Credit Watch™ Silver identity theft protection product

Equifax Credit Watch will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your Equifax credit file. The key features and benefits are listed below.

Equifax Credit Watch provides you with the following benefits:

- Comprehensive credit file monitoring of your Equifax credit report with daily notification of key changes to your credit file.
- Wireless alerts and customizable alerts available
- One copy of your Equifax Credit Report™
- $25,000 in identity theft insurance with $0 deductible, at no additional cost to you †
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalize identity theft victim assistance and in initiating an investigation of inaccurate information.
- 90 day Fraud Alert placement with automatic renewal functionality *
- Identity Restoration If you become a victim of identity theft, an Equifax identity restoration specialist will work on your behalf to help you restore your identity.

How to Enroll: You can sign up online

To sign up online for **online delivery** go to www.myservices.equifax.com/silver

1. Welcome Page: Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button.
2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.
3. Create Account: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the "Continue" button.
4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.
5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

Directions for placing a Fraud Alert

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your credit file, visit: www.fraudalerts.equifax.com or you may contact the Equifax auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf.

Information about Identity Theft Prevention

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for 7 years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax:	1-888-766-0008, www.equifax.com
Experian:	1-888-397-3742, www.experian.com

TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.