

WARCOG Frequently Asked Questions

What happened?

On or about June 28, 2017, the FBI notified Wooster-Ashland Regional Council of Governments (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.

When did it happen?

WARCOG became aware of the incident on or about June 28, 2017.

What personal information could have been accessed?

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.

Did you contact the police?

Yes. We reported the incident to the local police as well as the FBI and they are investigating.

Why was I notified?

The privacy and security of your personal information is very important and we wanted you to know about the possible exposure of your personal information. Also, some state laws require notification to potentially affected individuals.

How many other people are affected by this?

Approximately 123,000.

I do not work for WARCOG why was I notified?

This incident potentially affects individuals listed within police incident reports originating in the Cities of Wooster, Ashland, and Orrville over the last ten years. You were identified as such an individual.

Are you providing identity theft protection?

Yes. WARCOG is offering affected individuals an option to safeguard their credit. An individual can enroll in one year of free credit monitoring (2 years for CT residents per the request of the CT Attorney General) through Equifax[®] and its Credit Watch[™] Silver credit monitoring and identity theft protection product. The credit monitoring enrollment information and costs are discussed in the letter sent to you.

What are you doing to protect me?

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 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 now 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.

As stated in the letter that was sent to you, we have also arranged to have Equifax protect your identity for one year at no cost to you through its Credit Watch TM Silver credit monitoring and identity theft protection product.

Is the security or confidentiality of my personal information at risk at this time?

We believe that the vulnerability on our network has been secured and that your personal information is no longer accessible. We urge you to take advantage of the credit monitoring option discussed in the letter you received.

What do I do if I see suspicious activity in my bank account or credit file?

If you detect any suspicious activity in your bank account or credit file, you should contact your bank to report any suspicious activity, change online passwords and check your credit reports. Suspected fraud should also be reported to local law enforcement.

I think I may have been the victim of fraud. What should I do?

If you believe you have been the victim of fraud, we encourage you to contact law enforcement, and your card company or the financial institution that issued the card. We also encourage you to take advantage of the identity monitoring and identity protection services that we are making available through Equifax to any potentially affected client, free of charge for the next 12 months (24 months for CT residents).

Do I need to take any action?

We do not believe that you need to take any action other than monitoring your credit as outlined in the letter that was sent to you. We encourage you to take advantage of the Equifax option.