



Dear Participant:

Western Health Screening (“WHS”) is an organization that offers comprehensive blood screening tests. It partners with community organizations, such as hospitals, to provide onsite blood screenings at Health Fairs throughout the Western slope of Colorado. You have been a participant at Health Fairs in the past that were sponsored by either Montrose Memorial Hospital; Gunnison Valley Health; or Delta County Memorial Hospital (the “Hospitals”).

WHS recently learned that a vehicle owned by WHS in route to a Health Fair and passing through Salt Lake City, Utah, was stolen. There was a piece of computer equipment known as a “jump drive” belonging to WHS that was in the stolen vehicle. Upon learning of this theft, WHS immediately investigated and determined that the jump drive, which was password protected, but unencrypted, contained participants’ personal information. WHS learned of the theft on February 7, 2017, but determined that the jump drive was unencrypted on February 15, 2017. WHS is sending this letter to you as part of WHS’s, and the Hospitals’, commitment to privacy. We take privacy very seriously, and it is important to us that you are made fully aware of this incident.

When WHS learned of the theft, it immediately reported the theft to the Salt Lake City Police Department. The jump drive has not been recovered and the police continue to investigate. WHS also conducted its own internal investigation. WHS determined that the jump drive contained demographic information that had been collected by WHS for health fair participants from the years 2008-2012, including health fair participants’ names, addresses, phone numbers and in some instances Social Security numbers. WHS also determined that the jump drive can only be accessed via a unique password. The jump drive did not contain any medical information such as blood test results, nor did it contain any financial information such as credit card numbers or other source of payment information. To date, WHS has no evidence that any participants’ information was accessed by unauthorized persons or that any participants’ personal information has been misused.

We are notifying you out of an abundance of caution so that you can take appropriate steps to protect yourself. To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **kroll.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.

You have until July 14, 2017 to activate your identity monitoring services.

Membership Number:

To receive credit services by mail instead of online, or if you have questions about your identity monitoring services or need assistance with a fraud or identity theft issue please call Kroll at 1-855-781-0037, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. Please have your membership number ready. Additional information describing your services is included with this letter.

Even if you do not take advantage of the credit monitoring services, we encourage you to remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

Equifax	Experian	TransUnion
PO Box 740241	PO Box 9554	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-465-7166	1-888-397-3742	1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov
1-877-438-4338

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report if you believe your identity has been stolen or your personal information misused. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. WHS sincerely regrets that this incident occurred. WHS is committed to protecting your personal information. As a result of this incident, WHS has re-educated its employees with respect to safeguarding sensitive information and has taken steps to enhance its existing procedures related to storing and securing information on mobile devices.

You can contact WHS with questions and concerns, including to find out if your social security number was disclosed as part of this incident, in the following ways: (1) by calling WHS's toll free number (800) 410-3225, Monday thru Friday between the hours of 9:00 am and 4:00 pm MST; (2) by sending an email message to mywhs@westernhealthscreening.com; or (3) addressing a letter to our postal address: Western Health Screening, PO Box 30157, Billings, Montana 59107.

Sincerely,



Marge Hall, CEO
Western Health Screening



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services from Kroll:

Credit Monitoring through TransUnion

You'll receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your investigator can dig deep to uncover all aspects of the identity theft, and then work to resolve it.