

JDC Healthcare Management LLC

3030 Lyndon B Johnson Freeway
Suite 1400
Dallas, TX 75234

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

JDC Healthcare Management LLC (“JDC”) is writing to notify you of an incident that may have impacted the security of your personal information. We want to provide you with information about the incident, our response, and steps you may take to better protect against possible misuse of your personal information, should you feel it is necessary to do so.

What Happened? On or about August 9, 2021, JDC became aware of a malware incident impacting certain company systems. We immediately worked to restore our systems and launched an investigation, with assistance from third-party computer forensic specialists, to determine the nature and scope of the incident. Our investigation remains ongoing but determined that certain JDC data was subject to unauthorized access and/or acquisition during the incident between July 27, 2021 and August 11, 2021. Therefore, we conducted a comprehensive programmatic and manual review of the potentially impacted information to determine the type of information and to whom it related. On January 10, 2022, we completed this review and began obtaining contact information to notify potentially impacted individuals about this event. We also worked to engage additional services and resources for these individuals. Although we are unaware of any actual or attempted misuse of your personal information, we are providing you this notice out of an abundance of caution.

What Information Was Involved? The investigation determined that your <<b2b_text_1 (name[, / and][type(s) of impacted information]>><<b2b_text_2 (impacted data, cont.)>><<b2b_text_3 (impacted data, cont.)>> may have been accessed and/or acquired by an unauthorized individual.

What We Are Doing. We take this incident and the security of personal information in our care very seriously. Upon learning of this incident, we moved quickly to investigate and respond to this incident, assess the security of our systems, restore functionality to our environment, and notify potentially affected individuals. As part of our ongoing commitment to the security of information, we are reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event. As a precautionary measure, we are notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so. We regret any inconvenience or concern this incident may cause. As an added precaution, JDC is offering you access to twenty-four (24) months of free identity monitoring services through Kroll at no cost to you.

What You Can Do. Please review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains information on what you can do to better protect against possible misuse of your information. 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. You will also find information on how to activate the identity monitoring services offered.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at 855-568-2158 Monday through Friday, 8:00 am to 5:30 pm Central time, excluding major U.S. holidays.

We take the privacy and security of personal information in our care seriously, and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Mick McCormick
Chief Executive Officer

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Activate Identity Monitoring

You have been provided with complimentary access to the following services from Kroll:

Single Bureau Credit Monitoring

You will 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 will be able to help you determine if it is 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 can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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

You have until <<b2b_text_6 (Activation Date)>> to activate your identity monitoring services.

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.