## Below is the text of the July 8, 2019 notice regarding the AMCA data security incident:

Su información personal puede haber estado involucrada en un incidente de datos.
Si desea recibir una versión de esta carta en español, por favor llame 1-800-491-5304.

July 8, 2019 Notice
Unauthorized Access to Database at AMCA Containing Personal Information

Retrieval-Masters Creditors Bureau, Inc. (also known as American Medical Collection Agency ("AMCA")) has informed Quest Diagnostics Incorporated ("Quest") and Optum360, LLC ("Optum360") of an incident that may have affected personal information about you related to services you received at Quest. Optum360 provides revenue management services for Quest, and AMCA provided debt collection services for Optum360. This notice is not regarding collection of a debt, but rather to inform you about what happened regarding the AMCA incident, what information may have been involved, what we are doing in response to the incident, and what you can do. The incident affected AMCA's system which contained personal information concerning Quest accounts that were sent to AMCA for debt collection. Quest was among several laboratories and other entities whose customers were affected by the AMCA data security incident.

In June 2019, AMCA mailed notices to certain individuals whose information was contained on the affected AMCA system, including some individuals who are associated with services Quest provided. Quest and Optum360 are also mailing notices to additional individuals whose information may have been affected by the incident at AMCA and were not included in a June 2019 mailing by AMCA. As further described in those two sets of notices, complimentary credit monitoring is being offered to those recipients whose Social Security Numbers, credit card information or bank account numbers may have been involved. Since it is possible there may be insufficient or out-of-date contact information for some individuals whose information was contained on the affected AMCA system, this notice is also being posted on Quest's website consistent with the Health Insurance Portability and Accountability Act ("HIPAA").

---

### What Happened?

On May 14, 2019, AMCA informed Optum360 and Quest ("us" or "we") of potential unauthorized activity on AMCA's web payment page. AMCA subsequently informed us that it had learned, after an external forensics review, that an unauthorized user had access to AMCA's system between August 1, 2018 and March 30, 2019. The incident affected AMCA's system; neither Optum360's nor Quest's systems or databases were involved in the incident.

## What Information Was Involved?

AMCA has informed us that the information stored in the affected AMCA system included information relating to the laboratory services you received from Quest. This may have included: information used to identify and contact you (such as first, middle and last name, date of birth, Social Security Number, address, phone number); information related to your providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as credit card information, bank account number, insurance/payer information and identification number, diagnosis codes, internal account number). Test results were not included.

## What We Are Doing.

AMCA has informed us that it took down its web payments page and migrated it to a third-party vendor. AMCA has also informed us that it conducted an external forensic review, retained a computer security consulting firm to increase the security of AMCA's systems, and engaged with law enforcement.

Since learning of this incident, we have been working to determine what happened and what information was potentially affected as a result, and Optum360 retained a forensic expert to investigate the incident. On June 7, 2019, AMCA provided to Optum360 data regarding the population of Quest patients whose information may have been included in the affected AMCA system but who had not been notified by AMCA.

We have ceased using AMCA for collection services. On June 17, 2019, AMCA filed for bankruptcy. We understand AMCA now intends to wind down and liquidate its business.

For the next 90 days, Quest customers, including those individuals who received a June 2019 letter from AMCA, may call toll-free 1-800-491-5304 Monday through Friday from 8 a.m. to 5:30 p.m. Central Standard Time or visit https://amcaincident.kroll.com/ (https://amcaincident.kroll.com/) to ask questions and learn additional information. This substitute notice and toll-free number will remain active for at least 90 days.

## What You Can Do.

Monitoring. As a precautionary measure, you should remain vigilant for fraud and identity theft by reviewing and monitoring your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. Carefully review statements sent to you from healthcare providers as well as from your insurance company to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider's billing office, or for insurance statements, to your insurance company. You are also entitled to a free credit report every twelve months from each of the agencies listed below by visiting https://www.annualcreditreport.com/index.action (https://www.annualcreditreport.com/index.action) or calling the following toll free number: 1-877-322-8228. A printable, mailed version of the request form is available here: https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0093-annual-report-request-form.pdf. (https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0093-annual-report-request-form.pdf) Or, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies is provided below:

| | | |
|---|---|---|
| Equifax<br>Equifax Information Services LLC<br>P.O. Box 740241<br>Atlanta, GA 30374<br>1-00-685-1111<br>https://www.equifax.com/personal/credit-report-services/<br>(https://www.equifax.com/personal/credit-report-services/) | Experian<br>P.O. Box 4500<br>Allen, TX 75013 1-888-397-3742<br>https://www.experian.com/help<br>(https://www.experian.com/help) | TransUnion<br>Fraud Victim Assistance Division<br>P.O. Box 2000<br>Chester, PA 19016<br>1-800-916-8800 https://www.transunion.com/credit-help (https://www.transunion.com/credit-help) |

Identity Theft. Contact information for the Federal Trade Commission ("FTC") is included in this letter. 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 FTC, the Attorney General's office in your state and/or local law enforcement — they can provide information about preventing identity theft. You also have the right to file a police report regarding this breach. You should obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. You can contact the FTC and the three credit reporting agencies mentioned above to learn more about fraud alerts and security freezes: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); https://www.identitytheft.gov/ (https://www.identitytheft.gov/).

Fraud Alerts. Further, you may contact any one of the three credit bureaus listed above (Equifax, Experian, or TransUnion) and place a fraud alert on your credit report file. A fraud alert tells creditors that you may be the victim of identity theft, so creditors may take extra steps to validate your identity before opening a new account or changing your existing accounts (for that reason, it may delay obtaining credit). There are two types of fraud alerts 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. An initial fraud alert is free and stays on your credit report for at least one year. 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 seven years.

Security Freezes. You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge. Security freezes restrict access to your credit report, making it harder for identity thieves to open new accounts in your name. If you place a security freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a security freeze on your credit file at each of the three credit reporting agencies (Equifax, Experian, and TransUnion). For further information and to place a security freeze, contact each of the credit reporting agencies below:

- Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348, 1-800-349-9960, https://www.equifax.com/personal/credit-report-services (https://www.equifax.com/personal/credit-report- services)
- Experian Security Freeze, P.O. Box 9554, Allen, TX 75013, 1-888-397-3742, https://www.experian.com/help (https://www.experian.com/help)
- TransUnion, P.O. Box 160, Woodlyn, PA 19094, 1-888-909-8872, https://www.transunion.com/credit-freeze (https://www.transunion.com/credit-freeze)

  If you request a security freeze online or by phone, the agency must place the freeze within one business day. A security freeze remains in place until you ask the credit bureaus to temporarily lift it (so that a specific entity or individual can access your credit report) or remove it altogether. If you request a temporary lift or removal of the security freeze online or by phone, the agency must lift it within one hour. If you make your request to place, lift, or remove the freeze by mail, the agency must place, lift, or remove the freeze within three business days after it receives your request.

---

For More Information.

We take this matter and your privacy very seriously. If you have any questions or concerns, or would like additional information about the AMCA data security incident, please call toll-free 1-800-491-5304 Monday through Friday from 8 a.m. to 5:30 p.m. Central Standard Time. You can also visit https://amcaincident.kroll.com/ (https://amcaincident.kroll.com/) for a list of frequently asked questions about the AMCA incident.