▪

From: Sari Ratican <SRatican@fenwick.com>
Sent: Friday, October 25, 2024 2:17 PM
To: IDTheft
Subject: NOTICE OF DATA INCIDENT
Attachments: Maryland -- Quest Notification Letter (10.25.2024).pdf; Attachment -- Quest Template Notification Letter (10.25.2024).pdf

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Data breach

CONFIDENTIAL TREATMENT REQUESTED

To Whom It May Concern:

We represent Quest Diagnostics Incorporated ("Quest") located at 500 Plaza Drive, Secaucus, New Jersey 07094 and are writing to notify your office of an incident that may affect the security of personal data relating to twenty (20) Maryland residents. By providing this notice, Quest does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Incident
On August 8, 2024, Quest implemented a new electronic payment functionality related to its billing platform. As a result of an unforeseen coding misconfiguration, some Quest patients using the new functionality were misdirected to one (1) or more Quest invoices related to another patient instead of their own.

On August 27, 2024, Quest discovered the misconfiguration, quickly disabled the new functionality, and initiated an internal investigation including a thorough review of the relevant internal systems to identify the coding misconfiguration causing the incident. The vast majority of invoices available via the new functionality were not affected; however, invoices of 1,062 Quest patients (including twenty (20) Maryland residents) were inadvertently accessed by another Quest patient. Most patients had only one (1) invoice affected by this incident and such impacted invoice(s) was/were accessed by only one (1) other Quest patient.

The information potentially viewed by the other Quest patient varies and may include name, address, health data (such as referring physician, tests performed (but not test results), CPT codes), health insurance information (such as plan name), and billing data (such as invoice numbers). No test results, diagnosis codes, social security numbers, or financial account data (such as payment card or bank account number) were accessed by the other Quest patient.

Notice to Impacted Residents
Written notice of this incident was provided to impacted state residents on October 25, 2024. Such notice was provided in substantially the same form as the attached template letter.

Other Steps Taken and To Be Taken

In addition to conducting the internal investigation, Quest implemented additional security controls and safeguards designed to prevent a similar event from recurring in the future and is working with an external cybersecurity consultant to validate the fixed coding configuration before the intended functionality is reengaged.

To support the impacted patients, Quest established a dedicated call center and is providing twelve (12) months of Kroll, Inc.'s "Complete" identity monitoring services at no cost to impacted individuals. Among other services provided, impacted patients registering for the offered identity monitoring services will also receive credit monitoring, a current credit report, various monitoring scans (including "Web Watcher," "Public Persona," and "Quick Cash"), $1 million identity fraud loss reimbursement, and fraud consultation and identity theft restoration services.

Additionally, the written notification letters sent to all impacted patients include information on how to protect against identity theft and fraud including advising patients to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Quest also provided information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Quest also provided written notice of this incident to relevant state regulators.

Contact Information
Should you have any questions regarding this notification or other aspects of this incident, please contact me at (310) 434-5495.

Very truly yours,
Sari H. Ratican, Esq.
FENWICK & WEST LLP

Attachment

Sari H. Ratican (she/her)
Name Pronunciation: Sari rhymes with Mary Fenwick | Counsel | +1 310-434-5495<mailto:+1%20310-434-5495>
sratican@fenwick.com<mailto:sratican@fenwick.com>

Robinson+Cole

LINN F. FREEDMAN

One Financial Plaza, 14th Floor
Providence, RI 02903-2485
Main (401) 709-3300
Fax (401) 709-3399
lfreedman@rc.com
Direct (401) 709-3353

Also admitted in Massachusetts

Sent via email idtheft@oag.state.md.us

Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

October 29, 2024

RE: Breach Notification

Dear Attorney General Brown:

Please be advised that we represent Quest Health Solutions ("Quest Health") in regard to a security incident. Pursuant to Md. Code Ann. § 14-3501 et seq., we are reporting to you, on behalf of Quest Health, that Quest Health is notifying eight (8) Maryland residents of a breach of their personal information.

On July 11, 2024, Quest discovered that one of its employees was the victim of a sohisticated phishing scheme. Quest consulted with third-party cybersecurity specialists to assist with its response to the incident. After forensic and manual review of the affected email account, Quest determined that personal information of Maryland residents may have been affected on or about October 7, 2024.

The Maryland residents affected by this incident will receive a notice pursuant to Md. Code Ann. § 14-3504 on or about October 30, 2024. A sample notice is enclosed.

If you have any questions or need further information, please do not hesitate to contact me.

Sincerely,

Linn F. Freedman

Linn F. Freedman

Enclosure

Quest Health Solutions
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

October 30, 2024

RE: Your Protected Health Information

Dear :

We are writing to notify you that Quest Health Solutions ("Quest Health") was the victim of a sophisticated phishing attack that involved your personal information. This letter provides you with information on the actions that we have taken in response, resources available to you, and steps you can take to protect yourself.

What Happened?
On July 11, 2024, Quest discovered that one of its employees was the victim of a sophisticated phishing scheme. We consulted with third-party cybersecurity specialists to assist with our response to the incident. After forensic and manual review of the affected email account, Quest determined that protected health information may have been affected on or about October 7, 2024.

What Information Was Involved?
The information affected may have included your name and health information.

What Are We Doing?
We consulted with third-party cybersecurity specialists to assist with our response to and remediation of the incident.

What Can You Do?
For information and steps that you can take to protect yourself, see enclosure.

For More Information
If you have any questions or need any additional information, please call our dedicated call center at 1-800-405-6108. Representatives are available for 90 days from the date of this letter to assist you between the hours from Monday through Friday from 8:00 a.m to 8:00 p.m. Eastern Time, excluding holidays. Please call the dedicated call center at 1-800-405-6108 and be prepared to supply the fraud specialist with your unique code listed within.

Sincerely,

Adam Nadler, CEO

Additional Information

Monitor Medical Records

We recommend that you regularly review medical records and Explanation of Benefits (EOB) statements for any inaccuracies or unfamiliar charges and use online patient portals to access and verify health information periodically. We recommend that you be cautious about sharing personal or health information and report any suspicious activity immediately.

Monitor Your Accounts

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, GA 30374-0241 1-800-685-1111 www.equifax.com	Experian P.O. Box 9701 Allen, TX 75013-9701 1-888-397-3742 www.experian.com	TransUnion® P.O. Box 1000 Chester, PA 19016-1000 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.

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

For more information about identity theft and your tax records, we recommend that you visit the IRS Taxpayer Guide to Identity Theft at http://www.irs.gov. You may want to consider notifying the IRS that your tax records may be at risk by completing IRS Form 14039 (Identity Theft Affidavit) which can be located at http://www.irs.gov/pub/irs-pdf/f14039.pdf. You will need to send Form 14039 to the IRS along with a copy of your valid government-issued identification, such as a Social Security card, driver's license, or passport to the address on the form or by faxing to 1-855-807-5720.

Detailed below are a few things to keep in mind when filing Internal Revenue Service Form 14039:

- All documents, including your identification, must be clear and legible;
- The identity theft marker will remain on your file for a minimum of three tax cycles;
- Any returns containing your Social security number will be reviewed by the IRS for possible fraud; and,
- The marker may delay the processing of any legitimate tax returns.

You may also have the right to file or obtain a police report with your local law enforcement office if you believe you have been a victim of identity theft or fraud. Remember to remain vigilant in reviewing your account statements, monitoring your free credit reports, and for incidents of fraud or identity theft.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, 1-800-952-5225.

Maryland Residents: You may wish to contact the Attorney General, Consumer Protection Division, for more information at 200 St. Paul Place, Baltimore, MD 21202, by telephone at 410-528-8662 or 888-743-0023, or by email at Consumer@oag.state.md.us. You can also visit the Consumer Protection Division website at https://www.marylandattorneygeneral.gov/ for more information.

Oregon Residents: You may wish to contact the Attorney General's Consumer Protection Division by email at help@oregonconsumer.gov or by telephone at 877-877-9392. You may also visit https://www.doj.state.or.us/consumer-protection/ for more information.

Rhode Island Residents: You may wish to contact the Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 401-274-4400. Please note that there were 5 affected individuals residing in Rhode Island.

Texas Residents: Please note that there were 18 affected individuals residing in Texas.

00001020280000

P

FENWICK

730 Arizona Avenue
1st Floor
Santa Monica, CA 90401

Sari Heller Ratican
sratican@fenwick.com | 310.434.5495

CONFIDENTIAL TREATMENT REQUESTED

October 25, 2024

VIA ELECTRONIC MAIL
Attorney General Brian Frosch
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

Re: Notice of Data Incident

To Whom It May Concern:

We represent Quest Diagnostics Incorporated ("Quest") located at 500 Plaza Drive, Secaucus, New Jersey 07094 and are writing to notify your office of an incident that may affect the security of personal data relating to twenty (20) Maryland residents. By providing this notice, Quest does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Incident

On August 8, 2024, Quest implemented a new electronic payment functionality related to its billing platform. As a result of an unforeseen coding misconfiguration, some Quest patients using the new functionality were misdirected to one (1) or more Quest invoices related to another patient instead of their own.

On August 27, 2024, Quest discovered the misconfiguration, quickly disabled the new functionality, and initiated an internal investigation including a thorough review of the relevant internal systems to identify the coding misconfiguration causing the incident. The vast majority of invoices available via the new functionality were not affected; however, invoices of 1,062 Quest patients (including twenty (20) Maryland residents) were inadvertently accessed by another Quest patient. Most patients had only one (1) invoice affected by this incident and such impacted invoice(s) was/were accessed by only one (1) other Quest patient.

The information potentially viewed by the other Quest patient varies and may include name, address, health data (such as referring physician, tests performed (but not test results), CPT codes), health insurance information (such as plan name), and billing data (such as invoice numbers). No test results, diagnosis codes, social security numbers, or financial account data (such as payment card or bank account number) were accessed by the other Quest patient.

Notice to Impacted Residents

Written notice of this incident was provided to impacted state residents on October 25, 2024. Such notice was provided in substantially the same form as the attached template letter.

Other Steps Taken and To Be Taken

In addition to conducting the internal investigation, Quest implemented additional security controls and safeguards designed to prevent a similar event from recurring in the future and is working with an external cybersecurity consultant to validate the fixed coding configuration before the intended functionality is reengaged.

To support the impacted patients, Quest established a dedicated call center and is providing twelve (12) months of Kroll, Inc.'s "Complete" identity monitoring services at no cost to impacted individuals. Among other services provided, impacted patients registering for the offered identity monitoring services will also receive credit monitoring, a current credit report, various monitoring scans (including "Web Watcher," "Public Persona," and "Quick Cash"), $1 million identity fraud loss reimbursement, and fraud consultation and identity theft restoration services.

Additionally, the written notification letters sent to all impacted patients include information on how to protect against identity theft and fraud including advising patients to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Quest also provided information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Quest also provided written notice of this incident to relevant state regulators.

Contact Information

Should you have any questions regarding this notification or other aspects of this incident, please contact me at (310) 434-5495.

Very truly yours,

Sari H. Ratican, Esq.
FENWICK & WEST LLP

Attachment