[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

From: Moore, Desiree F. <Desiree.Moore@klgates.com>
Sent: Friday, October 23, 2020 6:20 PM
To: DOJ: Attorney General <attorneygeneral@doj.nh.gov>
Subject: Notice of Security Incident

EXTERNAL: Do not open attachments or click on links unless you recognize and trust the sender.

To whom it may concern:

Kindly note that I am legal counsel for Ascend Clinical LLC ("Ascend"). I write regarding a recent data

security incident at Ascend.

On or about May 31, 2020, Ascend detected certain anomalies in its data systems, including limited encrypted data. Upon a thorough investigation, Ascend determined that the individuals behind the encryption perpetrated a phishing scheme some weeks prior (unbeknownst to Ascend) that ultimately enabled them to access select personal information relating to Ascend employees. Ascend internal teams worked diligently with forensic consultants to restore and secure the impacted systems. This included the installation of forensic tools on all systems and the isolation of impacted systems until Ascend could confirm that they were secure. Ascend also implemented additional countermeasures to block further ransomware emails from entering the environment and further upgraded its security measures to prevent future attacks.

On or about September 23, 2020, after a quality control review, it was determined that certain additional information may have been accessed by the threat actors. This information concerned patients of Ascend, including 20 New Hampshire residents. Those residents will be notified on or before October 26, 2020.

A sample notification is attached.

If you have any questions or require any additional information, please do not hesitate to contact me directly. Thank you.

Best regards,

Desiree

Desiree Moore
Partner
K&L Gates LLP
desiree.moore@klgates.com

70 W. Madison St.
Suite 3100
Chicago, IL 60602
Phone: +1 312 781 6028

www.klgates.com

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

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

Notice of Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to you, a patient who has received laboratory testing services from Ascend Clinical ("Ascend"). Ascend is a clinical reference laboratory specializing in testing services for kidney disease. Ascend experienced a data security incident that may have exposed some of your personal information.

For this reason, we are contacting you directly to explain the circumstances of the incident, although we have not received any indication that the information has been used by any unauthorized individual.

What happened?

On or about May 31, 2020, Ascend detected irregularities in its data systems, including some Ascend data that had become encrypted through an unknown source. Upon a thorough investigation, Ascend determined that an unauthorized user had accessed and downloaded Ascend business records, including some personally identifiable information ("PII") of Ascend's patients. Under a federal law known as the Health Insurance Portability and Accountability Act ("HIPAA"), this PII is considered protected health information ("PHI").

Ascend has notified federal and local law enforcement authorities and retained a leading third party cybersecurity firm to investigate the nature and scope of the incident. Ascend is also in the process of notifying state and federal agencies responsible for enforcing privacy laws, as required by law.

What information was involved?

The individuals behind the data security incident gained access to and downloaded files containing PII and PHI. At no time did the unauthorized users access Ascend's electronic health records, where the majority of Ascend's PHI was stored.

The information that may have been compromised includes your name and address, and may also include medical diagnosis, medical conditions, medical record number, medication, medication dosage, and/or your social security number. **Please note that this incident did not impact the accuracy of your test results in any way.**

What we are doing.

Ascend internal teams worked diligently with forensic consultants to restore and secure the impacted systems. This included the installation of forensic tools on all systems and the isolation of impacted systems until Ascend could confirm that they were secure. Ascend also implemented countermeasures and further upgraded its security systems to prevent future incidents such as this from occurring.

Ascend has 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 **https://enroll.idheadquarters.com** to take advantage of your identity monitoring services.

*You have until **<<Date>>** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing services available to you is included with this letter.

What you can do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help safeguard yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

Sincerely,

Cynthia Hoen
Compliance Officer

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 119016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. 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. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert 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 and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.