LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

July 15, 2019

VIA EMAIL
Attorney General Bob Ferguson
Office of the Attorney General
Consumer Protection Division
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100
Email: SecurityBreach@atg.wa.gov

Re: Notification of Data Security Incident

Dear Attorney General Ferguson:

We represent Clinical Pathology Laboratories, Inc. ("CPL") in connection with a recent data security incident experienced by a business associate of CPL, Retrieval Masters Creditors Bureau d/b/a American Medical Collection Agency ("AMCA"). The incident may have involved the personal information of CPL patients, and CPL is in the process of notifying its patients of the incident.

1. Nature of the security incident.

AMCA is a business associate of CPL that assisted with the collection of unpaid accounts. On May 15, 2019, CPL was notified that AMCA had experienced a data security incident that involved the payment page on AMCA's website. AMCA later advised CPL that the incident also involved unauthorized access to an AMCA database containing information belonging to CPL's patients. According to AMCA, it became aware of facts indicating there had been a data security incident on March 21, 2019, and after conducting an investigation, notified CPL almost two months later.

At the time of AMCA's initial notification, AMCA did not provide CPL sufficient information for CPL to identify its potentially affected patients or confirm the nature of patient information potentially involved in the incident. After receiving the initial notification from AMCA, CPL began an investigation to determine the identity of the affected individuals and nature of affected information. CPL also engaged cybersecurity experts to assist with the investigation. Based on the information provided by AMCA and as a result of CPL's investigation, the following personal information belonging to CPL patients may have been affected by the incident: patient name, address, phone number, date of birth, date(s) of service, balance information, and treatment provider information. AMCA has advised CPL that its patients' social security numbers were not involved in the incident. Additionally, CPL does not provide AMCA healthcare records such as laboratory results and clinical history.

AMCA informed CPL that there were some patients whose payment card or financial account information may have been impacted by this incident. AMCA has previously sent those patients notification letters.

Although CPL is not aware of any misuse of patient information involved in the incident, CPL also provided notification to the CPL patients who were not notified by AMCA about the incident and whose personally identifiable information may have been affected by the incident.

2. Number of Washington residents affected.

CPL is in the process of notifying 1,155 Washington residents regarding this data security incident. Notification letters are being mailed via first class U.S. mail beginning on July 15, 2019. A sample copy of the notification letter is included with this letter.

3. Steps taken relating to the incident.

CPL takes the security of its patients' information very seriously, including the security of data handled by its business associates. As a result of the incident, CPL is no longer using AMCA for collection efforts.

4. Contact information.

CPL is dedicated to protecting the sensitive information that is in its control. If you have any questions or need additional information, please do not hesitate to contact me at (214) 722-7141, or by e-mail at Lindsay.Nickle@LewisBrisbois.com.

Sincerely,

Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure

CLINICAL PATHOLOGY LABORATORIES
C/O ID Experts
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Data Security Incident

Dear <<Name 1>>:

We are writing to inform you of a data security incident experienced by Retrieval Masters Creditors Bureau d/b/a American Medical Collection Agency ("AMCA"), one of Clinical Pathology Laboratories, Inc.'s ("CPL") vendors. This incident may have involved your personal information. At CPL we take the privacy and security of our patients' information very seriously. We are sending you this letter to notify you about the incident and provide information about steps you can take to protect your information.

What Happened?

On May 15, 2019, we were notified that AMCA experienced a data security incident that involved the payment page on AMCA's website and unauthorized access to an AMCA database containing information belonging to CPL's patients. AMCA is a vendor that assisted CPL with the collection of unpaid accounts. The security of CPL's systems was not affected by this incident. Upon receiving notification about this incident, we immediately began an investigation to identify the affected individuals and the nature of affected information. We are utilizing cyber security experts to assist us in our investigation. Although we are unaware of the misuse of any of your personal information, out of an abundance of caution, we are notifying you about this incident and providing you information about steps you can take to protect your personal information.

What Information Was Involved?

Your name, address, phone number, date of birth, date(s) of service, balance information, and treatment provider information may have been involved in the incident.

What We Are Doing And What You Can Do.

Since receiving notification about the incident, CPL has stopped using AMCA for collection efforts. In addition, although we are not aware of any misuse of your information, we are providing you with this notification about the incident. The following pages also include information about steps you can take to protect your personal information as a precautionary measure.

For More Information.

The privacy and protection of patient information is a top priority at CPL, and we appreciate your patience and loyalty through this incident. If you have any questions, please do not hesitate to call 833-300-6927 from 9:00 a.m. to 9:00 p.m., Eastern Time, Monday through Friday or you can go to the informational website at https://ide.myidcare.com/CPL.

Please be advised that effective immediately, payments should no longer be made to AMCA. If you have an outstanding balance, please contact us directly at 800-411-2762.

Sincerely,

Bobby Smithson
President

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant for the next twelve to twenty-four months and review 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. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. If you detect any information related to fraudulent transactions, you should notify the credit reporting agency that issued the report and have it deleted. You can also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You are encouraged to report suspected identity theft to the FTC. You may also report suspected identity theft to local law enforcement, including the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: https://www.consumer.ftc.gov/articles/0040-child-identity-theft.