WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

STATE OF NH
DEPT OF JUSTICE
2021 SEP -7 P 1:14

September 3, 2021

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Certified Mail; Return Receipt Requested

Attorney General John Formella
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

Re: Cybersecurity Incident Involving K&B Surgical Center LLC

Dear Attorney General Formella:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents K and B Surgical Center, LLC ("K&B"), a surgical center located in 9033 Wilshire Boulevard, Suite 210, Beverly Hills, CA 90211, with respect to a recent cybersecurity incident that was first discovered by K&B on March 30, 2021 (hereinafter, the "Incident"). K&B takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of New Hampshire residents being notified, and the steps that K&B has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On March 30, 2021, K&B discovered that an unauthorized user had gained access to its network. Upon discovery of this incident, K&B promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. On April 27, 2021, the forensic investigation determined that an unauthorized user accessed K&B's systems from March 24, 2021 to March 30, 2021. Then K&B performed data mining on the affected servers to identify the specific individuals and the types of information that may have been compromised. On July 27, 2021, K&B finalized the list of individuals to notify.

Although K&B is unaware of any fraudulent misuse of information, it is possible that individuals' full name, address, phone number, driver's license number, and protected health information, including, but not limited to, medical diagnosis, treatment and prescription information, provider name, patient ID, Medicare/Medicaid number, lab results, health insurance information, and treatment cost information may have been exposed as a result of this unauthorized activity.

As of this writing, K&B has not received any reports of related identity theft since the date of the incident (March 30, 2021 to present).

2. Number of New Hampshire residents affected.

K&B identified and notified 14,772 individuals potentially affected by this Incident. Of those, five (5) were residents of New Hampshire. Notification letters to these individuals were mailed on September 3, 2021, by first class mail. A sample copy of the notification letters sent to New Hampshire residents is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

K&B is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, K&B moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Specifically, K&B engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, K&B changed passwords for all user accounts, VPN connections, and emails, installed new anti-virus security systems and threat monitoring programs on all computers, implemented periodic network security audits, re-trained employees on security, and updated the security rule risk analysis. Lastly, K&B informed our law firm and began identifying the potentially affected individuals in preparation for notice.

Although K&B is not aware of any actual or attempted misuse of the affected personal information, K&B offered 12 months of complimentary credit monitoring and identity theft restoration services through Equifax to all individuals to help protect their identity. Additionally, K&B provided guidance on how to better protect against identity theft and fraud, including providing 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 the contact details for the Federal Trade Commission.

4. Contact information

K&B remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

EXHIBIT A

K|B Surgical Center

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

Via First Class Mail

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

<<Date>>

Notice of Data Breach

Dear <<Name 1>>,

K and B Surgical Center, LLC ("K&B") is writing to inform you of a recent data security incident that may have resulted in an unauthorized access of your sensitive personal information. While we are unaware of any misuse of your personal information at this time, we are providing you with details about the event, steps we are taking in response, and free resources available to help you protect your information.

What Happened?

On March 30, 2021, K&B discovered that an unauthorized user had gained access to its network. Upon discovery of this incident, K&B promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. On April 27, 2021, the forensic investigation determined that an unauthorized user accessed K&B's systems from March 24, 2021 to March 30, 2021. Then K&B performed data mining on the affected servers to identify the specific individuals and the types of information that may have been compromised, and on July 27, 2021, K&B finalized the list of individuals to notify. At this time, K&B has no reason to believe your personal information has been misused by any third parties. However, out of an abundance of caution, K&B wanted to inform you of this incident.

What Information Was Involved?

The types of information involved varied by individual. However, the information potentially exposed during the unauthorized access may have included your name, date of birth, <<data elements>>.

What We Are Doing

K&B is committed to ensuring the privacy and security of all personal information in our care. Since the discovery of the incident, K&B have taken and will continue to take steps to mitigate the risk of future issues. Specifically, K&B engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. K&B also changed passwords for all user accounts, VPN connections, and emails, installed new anti-virus security systems and threat monitoring programs on all computers, implemented periodic network security audits, re-trained employees on security, and updated the security rule risk analysis. Additionally, K&B is providing you with guidance on how to help protect against the possibility of information misuse.

Furthermore, K&B is providing you with 12 months of complimentary identity monitoring services through Equifax. While K&B is covering the cost of these services, you will need to complete the activation process by following the instructions included in the enclosed *Steps You Can Take to Help Protect Your Information*.

What You Can Do

K&B encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and take the recommended steps to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information* to learn more about how to protect against the possibility of information misuse.

You may also activate the identity monitoring services we are making available to you. Again, while K&B is providing these services to you at no cost, you will need to activate these services yourself. The activation deadline is <<enrollment deadline>>.

K&B would like to reiterate that, at this time, there is no evidence that your information was misused. However, K&B encourages you to take full advantage of the services offered.

For More Information

K&B recognizes that you may have questions not addressed in this letter. If you have additional questions, please call 800-620-7091 (toll free) during the hours of 6 a.m. and 6 p.m. Pacific Standard Time, Monday through Friday (excluding U.S. national holidays).

K&B sincerely regrets any inconvenience or concern that this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Dr. Theodore Khalili
Managing Partner
K and B Surgical Center, LLC

Steps You Can Take to Help Protect Your Information

Credit Monitoring Enrollment Instructions (Note: You must be over age 18 with a credit file to take advantage of the product)

Go to www.equifax.com/activate and enter your unique Activation Code of <<ACTIVATION CODE>> then click "Submit" and follow these 4 steps:

1. ***Register***: Complete the form with your contact information and click "Continue".
   a. If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. ***Create Account***: Enter your email address, create a password, and accept the terms of use.
3. ***Verify Identity***: To enroll in your product, we will ask you to complete our identity verification process.
4. ***Checkout***: Upon successful verification of your identity, you will see the Checkout Page. Click 'Sign Me Up' to finish enrolling.

You're done! The confirmation page shows your completed enrollment. Click "View My Product" to access the product features.

Credit Monitoring Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Additional Important Information

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

---

[1] *WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.*

[2] *The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.*

[3] *Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.*

[4] *The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

Security Freeze: You also have the right to place a security freeze on your credit report. 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 need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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 five 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, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

More information can also be obtained by contacting the Federal Trade Commission:
Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580;1-877-IDTHEFT (438-4338);www.identitytheft.gov.

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Colorado, Illinois, Iowa, Maryland, Missouri, New Mexico, North Carolina, Oregon*, and *West Virginia*: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

***For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina*, and *Rhode Island*:** You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.
Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov
Arizona Office of the Attorney General - Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025
Colorado Office of the Attorney General - Consumer Protection, 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov
District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov
Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov
Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us
New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft
North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com
Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence, RI 02903; 1-401-274-4400; www.riag.ri.gov