Representing Management Exclusively in Workplace Law and Related Litigation

jackson lewis.

Jackson Lewis P.C.
220 Headquarters Plaza
East Tower, 7th Floor
Morristown, NJ 07960-6834
Tel 973 538-6890
Fax 973 540-9015
www.jacksonlewis.com
Richard J. Cino - Managing Principal

ALBANY, NY	GREENVILLE, SC	MONMOUTH COUNTY, NJ	RALEIGH, NC
ALBUQUERQUE, NM	HARTFORD, CT	MORRISTOWN, NJ	RAPID CITY, SD
ATLANTA, GA	HONOLULU, HI*	NEW ORLEANS, LA	RICHMOND, VA
AUSTIN, TX	HOUSTON, TX	NEW YORK, NY	SACRAMENTO, CA
BALTIMORE, MD	INDIANAPOLIS, IN	NORFOLK, VA	SALT LAKE CITY, UT
BIRMINGHAM, AL	JACKSONVILLE, FL	OMAHA, NE	SAN DIEGO, CA
BOSTON, MA	KANSAS CITY REGION	ORANGE COUNTY, CA	SAN FRANCISCO, CA
CHICAGO, IL	LAS VEGAS, NV	ORLANDO, FL	SAN JUAN, PR
CINCINNATI, OH	LONG ISLAND, NY	PHILADELPHIA, PA	SEATTLE, WA
CLEVELAND, OH	LOS ANGELES, CA	PHOENIX, AZ	ST. LOUIS, MO
DALLAS, TX	MADISON, WI	PITTSBURGH, PA	TAMPA, FL
DAYTON, OH	MEMPHIS, TN	PORTLAND, OR	WASHINGTON, DC REGION
DENVER, CO	MIAMI, FL	PORTSMOUTH, NH	WHITE PLAINS, NY
DETROIT, MI	MILWAUKEE, WI	PROVIDENCE, RI	
GRAND RAPIDS, MI	MINNEAPOLIS, MN		

*through an affiliation with Jackson Lewis P.C., a Law Corporation

February 20, 2018

Via First Class Mail and Email (Idtheft@oag.state.md.us)
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: **Data Incident Notification**

Dear Attorney General Frosh:

Please be advised, on January 23, 2018, our client, Rockville Eye Surgery Center, LLC d/b/a Palisades Surgery Center ("Palisades") learned that personal information may been subject to unauthorized access or acquisition as the result of a cyber-attack. The data elements involved may have included name, address, Social Security number, and medical information.

Immediately upon learning of the incident, Palisades commenced an investigation to determine the scope of this incident and identify those affected. With the assistance of third-party forensic experts, Palisades conducted a review of its systems in an effort to ensure the incident did not result in any additional exposure to personal information and took steps to confirm the integrity of Palisades' electronic systems. It appears that 10 patients or prospective patients could have been affected, including 2 Maryland residents. In light of this incident, Palisades plans to begin notifying the affected individuals in the next several days. A draft copy of the notification that will be sent is attached.

As set forth in the attached letter, Palisades has taken numerous steps to protect the security of the personal information of the affected individuals. In addition to continuing to monitor this situation, Palisades is reexamining its current privacy and data security policies and procedures to find ways of reducing the risk of future data incidents. Palisades will also be reviewing its technical security policies and procedures and making improvements where it can to minimize the chances of this happening again. Should Palisades become aware of any significant developments concerning this situation, we will inform you.

If you require any additional information on this matter, please call me.

Sincerely,

JACKSON LEWIS P.C.

Jason C. Gavejian

Encl.
4812-1779-0045, v. 1

[[COMPANY] LOGO]

[Return Address]

[NAME]
[ADDRESS

[DATE]

Dear [NAME]:

On January 23, 2018, Rockville Eye Surgery Center, LLC d/b/a Palisades Surgery Center ("Palisades") learned that your personal information may been subject to unauthorized access or acquisition as the result of a cyber-attack. The data elements involved may have included name, address, and medical information. Your Social Security number was not involved in this incident. We are sending this advisory to you so that you can take steps to protect yourself and minimize the possibility of misuse of your information. We apologize for any inconvenience this may cause you and assure you we are working diligently to resolve this incident.

Immediately upon learning of the incident, we commenced an investigation to determine the scope of this incident and identify those affected. With the assistance of third-party forensic experts, we conducted a review of our systems in an effort to ensure the incident did not result in any additional exposure to personal information and took steps to confirm the integrity of Palisades' electronic systems. Notwithstanding these steps, set forth below are additional steps you can take to protect your identity, credit, and personal information.

We treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. We continue to assess and modify our privacy and data security policies and procedures to prevent similar situations from occurring. Theft of data and similar incidents are difficult to prevent in all instances, however, we will be reviewing our systems and making improvements where we can to minimize the chances of this happening again.

If you have questions or concerns you should call [Insert Number] from [Hours]. Again, we apologize for this situation and any inconvenience it may cause you.

Sincerely,

[Insert name and title]

What You Should Do to Protect Your Personal Information

We recommend you remain vigilant and consider taking one or more of the following steps to avoid identity theft, obtain additional information, and protect your personal information:

1. Contacting the nationwide credit-reporting agencies as soon as possible to:

- Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. To place a 90 day fraud alert on your credit file, log into the Equifax Member Center and click on the fraud alert tab, visit www.fraudalerts.equifax.com or call the auto fraud line at 1-877-478-7625, and follow the simple prompts. This fraud alert will remain on your credit file for 90 days.
- Place a "security freeze" on your credit account. This means that your credit account cannot be shared with potential creditors. A security freeze can help prevent new account identity theft. If you would like to request a security freeze be placed on your account, you must write by certified or overnight mail (see addresses below) to each of the three credit reporting agencies, or through the electronic or Internet method made available by the credit reporting agencies. Credit reporting agencies charge a $5 fee to place or remove a security freeze, unless you provide proof that you are a victim of identity theft, in which case there is no fee. A copy of your police report or an investigative report or written FTC complaint documenting identity theft must be included to avoid a fee. In your request, you also must include (documentation for both the spouse and the victim must be submitted when requesting for the spouse's credit report) (i) a copy of either the police report or case number documenting the identity theft, if you are a victim of identity theft; (ii) your full name (including middle initial

as well as Jr., Sr., II, III, etc.,) address, Social Security number, and date of birth; (iii) if you have moved in the past 5 years, the addresses where you have lived over the prior 5 years; (iv) proof of current address such as a current utility bill or phone bill; (v) a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and, if applicable (vi) payment by check, money order or credit card (Visa, Master Card, American Express or Discover cards only.)

- Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
- Receive a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 2390	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(866) 510-4211	(866) 751-1323	(800) 888-4213
psol@equifax.com	databreachinfo@experian.com	https://tudatabreach.tnwreports.com/
www.equifax.com	www.experian.com/	www.transunion.com

2. Contacting the Federal Trade Commission ("FTC") either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you can report this to the Fraud Department of the FTC, who will collect all information and make it available to law-enforcement agencies. Contact information for the FTC is:

   Federal Trade Commission
   Consumer Response Center
   600 Pennsylvania Avenue
   NW Washington, DC 20580

3. If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

4. If you believe you are a victim of identity theft you should immediately report same to law enforcement and/or your state attorney general.

5. *For Maryland Residents*: The contact information for the Maryland Office of the Attorney General is: Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; Telephone: (888) 743-0023; website: http://www.oag.state.md.us.