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

JASON C. GAVEJIAN
JASON.GAVEJIAN@JACKSONLEWIS.COM

June 1, 2018

VIA OVERNIGHT MAIL
Office of Attorney General
Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: **Data Incident Notification**[7]

Dear Sir/Madam:

Please be advised that on May 22, 2018, our client, Stein Eriksen Lodge Hotel (the "Hotel") learned that personal information of state residents may have been subject to unauthorized access or acquisition as the result of a cyber-attack. Based on the investigation, it appears the attack occurred between September 9, 2017 and January 24, 2018. The data elements involved may have included name, address, birth date, and Social Security number.

Immediately upon discovering the intrusion, the Hotel commenced an investigation to determine the scope of this incident and identify those affected. The Hotel worked with its information technology team to conduct a thorough scan of its systems in an effort to ensure the attack did not result in any additional exposure to personal information and took steps to confirm the integrity of the Hotel's electronic systems. The Hotel also worked with forensic experts to determine what information may have been accessed. It appears that 1992 individuals could have been affected, including 4 residents of New Hampshire. In light of this incident, the Hotel plans to notify the affected individuals in the next several days. A draft copy of the notification that will be sent is attached.

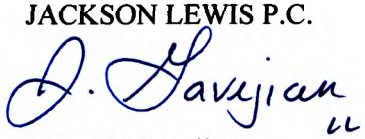
As set forth in the attached letter, the Hotel has taken numerous steps to protect the security of the personal information of the affected individuals. In addition to this notice, the Hotel has reported this incident to the Federal Bureau of Investigation ("FBI") and the local police. In addition to continuing to monitor this situation, the Hotel is reexamining its current data privacy and security policies and procedures to find ways of reducing the risk of future data incidents. Should the Hotel become aware of any significant developments concerning this situation, we will inform you.

[7] Please note that by providing this letter the Hotel is not agreeing to the jurisdiction of State of New Hampshire, or waiving its right to challenge jurisdiction in any subsequent actions.

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

Sincerely,

JACKSON LEWIS P.C.



Jason C. Gavejian

Enclosure

4820-3238-4359, v. 1

Company Logo

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

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

Dear <<Name 1>>:

On May 22, 2018, Stein Eriksen Lodge Hotel (the "Hotel") learned that your personal information may have been subject to unauthorized access or acquisition as the result of a cyber-attack. This information was maintained by the Hotel in connection with your current or past employment with the Hotel. Based on the investigation, it appears the attack occurred between September 9, 2017 and January 24, 2018. The data elements involved may have included name, address, birth date, and Social Security number. 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 discovering the intrusion, we commenced an investigation to determine the scope of this incident and identify those affected. We worked with our information technology team to conduct a thorough scan of our systems in an effort to ensure the attack did not result in any additional exposure to personal information and took steps to confirm the integrity of the Hotel's electronic systems. We also worked with forensic experts to determine what information may have been accessed. We have reported this incident to the Federal Bureau of Investigation ("FBI") and the local police. This communication was not delayed at the request of law enforcement. Notwithstanding these steps, set forth below are additional steps you can take to protect your identity, credit, and personal information.

As an added precaution, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion® , one of the three nationwide credit reporting companies. **To receive these services you must enroll by [INSERT], 2018.**

To enroll in this service, go to the myTrueIdentity website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the Activation Code provided at the top of this letter, and follow the three steps to receive your credit monitoring service online within minutes. If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code **[CODE]** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

We treat all sensitive employee 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. Attorney General contact information may be found at: http://www.naag.org/naag/attorneys-general/whos-my-ag.php.

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.

6. *For Massachusetts Residents:* You have the right to obtain a police report relating 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.

7. For *North Carolina Residents*: The contact information for the North Carolina Attorney General is: Address: North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699; Telephone: (919) 716-6400; website: ncdoj.com/.

8. *For Rhode Island Residents*: The contact information for the Rhode Island Office of the Attorney General is: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903; Telephone: (401) 274-4400; website: http://www.riag.ri.gov. The total number of affected individuals is currently unknown.

9. *For New Mexico Residents*: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have 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 or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to http://consumersunion.org/pdf/security/securityNM.pdf