Representing Management Exclusively in Workplace Law and Related Litigation

jackson lewis.

Jackson Lewis P.C.
200 Connell Drive, Suite 2000
Berkeley Heights, New Jersey 07922
Tel 908 795-5200
www.jacksonlewis.com
Richard J. Cino - Managing Principal

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

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

JASON C. GAVEJIAN, ESQ.
Direct Dial: (908) 795-5139
Email: Jason.Gavejian@jacksonlewis.com

April 24, 2020

VIA ELECTRONIC MAIL
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
Email: consumer@ag.iowa.gov

Re: Data Incident Notification[1]

Dear Attorney General Miller:

Please be advised that on April 9, 2020, our client, Spencer Municipal Hospital (the "Hospital"), learned that personal information of state residents may have been subject to unauthorized access or acquisition as the result of a cyberattack which occurred at PaperlessPay, a third-party vendor of the Hospital (the "Incident"). Based on the investigation, which we understand was conducted by PaperlessPay and in coordination with the Federal Bureau of Investigation ("FBI") and the Department of Homeland Security ("DHS"), it appears the Incident occurred at the vendor sometime on or before February 18, 2020. The data elements involved may have included name, address, earnings, and Social Security number. This information was maintained by the Hospital, and subsequently the vendor, in connection with individuals' current or former employment with the Hospital.

Immediately upon learning about the Incident, the Hospital sought to determine the scope of the Incident and identify those affected. This included working with its internal team and the third-party vendor to ensure the Incident did not result in any additional exposure to personal information. The Hospital also worked with PaperlessPay to determine what information may have been at risk.

Our understanding is that PaperlessPay's investigation (including work by the FBI and/or DHS) determined that the unauthorized actor may have gained access to a server of the vendor, which contained the Hospital's data, but was unable to determine what information contained within the drive was accessed or acquired as a result of this Incident. Nevertheless, the Hospital requested from PaperlessPay, and received, a list of the all individuals associated with the Hospital whose personal information may have been potentially impacted by the Incident. It appears that 747 individuals could have been affected, including 727 Iowa residents.

In light of this Incident, the Hospital plans to begin notifying individuals in the next several days. The Hospital will also provide one year of free credit monitoring to all affected individuals. A draft copy of the notification that will be sent is enclosed with this letter.

[1] Please note that by providing this letter the Hospital is not agreeing to the jurisdiction of State of Iowa, nor waiving its right to challenge jurisdiction in any subsequent actions.

As set forth in the enclosed letter, the Hospital has taken numerous steps to protect the security of the personal information of all individuals. In addition to continuing to monitor this situation, the Hospital is reexamining its current privacy and data security, policies and procedures to find ways of reducing the risk of future data incidents. The Hospital is also reviewing its technical security policies and procedures and making improvements where it can to minimize the chances of this happening again. Should the Hospital 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.

s/ Jason C. Gavejian
Jason C. Gavejian

JCG:tcm
Encl.
4813-2554-0026, v. 1

Spencer Hospital
1200 First Avenue East
Spencer, Iowa 51301

[Date]

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

Dear _____:

We recently learned that PaperlessPay Corporation ("PaperlessPay"), the owner and operator of eStubview and a third-party vendor of Spencer Municipal Hospital (the "Hospital"), was subjected to a data security incident as the result of a cyberattack (the "Incident"). This vendor supplies the website for your online access to bi-weekly payroll checkstub information and the annual IRS W-2 Forms. We are writing to inform you that some of your personal information may have been subject to unauthorized access or acquisition as the result of that Incident. This information was maintained by the Hospital, and subsequently the vendor, in connection with your current or former employment. While we are not aware of any misuse of your information, we are providing this notice to inform you of the Incident and to call your attention to steps you can take to help protect yourself and your personal information. We apologize for any inconvenience this may cause you and assure you that we have worked diligently to resolve this matter and continue to deploy measures to avoid these types of incidents from occurring in the future. Below you will also find instructions and a code redeemable for one year of credit monitoring with Experian, which the Hospital is making available at no cost to you.

What Happened?
On April 9, 2020, the Hospital was informed that your personal information may have been accessible to an unauthorized actor as a result of the Incident. Based on the investigation, it appears the Incident occurred at the vendor sometime on or before February 18, 2020. We have no reason to believe that any of the Hospital's systems were compromised, the Incident only occurred on the systems of this third-party vendor.

What Information Was Involved?
The personal information subject to this Incident may have included personal information such as your name, address, earnings, and Social Security number.

What We Are Doing.
The Hospital values your privacy, and immediately upon learning about the Incident we sought to determine the scope of the Incident and identify those affected. This included working with our internal team and PaperlessPay, who conducted their own investigation in coordination with the Federal Bureau of Investigation ("FBI") and the Department of Homeland Security ("DHS"), to ensure the Incident did not result in any additional exposure to personal information. The Hospital also worked with PaperlessPay to determine what information may have been at risk. The Hospital will notify you if it becomes aware of any significant developments.

As mentioned, the Federal Bureau of Investigation ("FBI") and the Department of Homeland Security ("DHS") are aware of the Incident. This communication was not delayed at the request of law enforcement.

As an added precaution, we have arranged for credit monitoring and identity restoration services to be provided to you by Experian at no cost to you. If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for one year from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks^{SM} as a complimentary one-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **[date]** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **[URL]**
- Provide your **activation code**: **[code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **[customer service number]** by **[enrollment end date]**. Be prepared to provide engagement number **[engagement number]** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12 MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.

- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What You Can Do.
In addition to taking advantage of the credit monitoring and identity restoration services outlined above, there are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to the below and www.ExperianIDWorks.com/restoration for this information.

Other Important Information.
We treat all personal 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. Unauthorized access to personal information and similar incidents are difficult to prevent in all instances; however, we will continue reviewing our systems and making improvements where we can to minimize the chances of this happening again.

For More Information.
For more information, for further assistance, or 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,

Bill Bumgarner
CEO/President
Spencer Hospital

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. 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.
- 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. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. You may contact the FTC by visiting www.ftc.gov or www.consumer.gov/idtheft, calling (877) 438-4338, or writing to the FTC at the address below. If you suspect or know that you are the victim of identity theft, you should contact local police and/or your state Attorney General. You can also report such activity to the Fraud Department of the FTC, which will collect all relevant information and make it available to law-enforcement agencies. The mailing address 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. The IRS also offers Identity Protection: Prevention, Detection and Victim Assistance which can be found at: https://www.irs.gov/Individuals/Identity-Protection.

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

6. *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: www.ncdoj.com/.