



May 4, 2023

Via electronic-mail: DOJ-CPB@doj.nh.gov

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: **Client: McPherson Hospital, Inc.**
Matter: Notice of Data Security Incident

Dear Attorney General:

We represent McPherson Hospital, Inc. (“McPherson”), which is located in McPherson, Kansas. Our representation of McPherson relates to a data security incident described in more detail below. McPherson takes the security and privacy of the information in its control 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 security incident, the number of New Hampshire residents being notified, what information has been compromised, and the steps that McPherson has taken to restore the integrity of the system. We have also enclosed a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring.

Nature of the Security Incident

On July 12, 2022, McPherson detected and stopped a sophisticated ransomware attack, in which an unauthorized third party accessed and disabled some of McPherson’s computer systems. McPherson immediately engaged third-party forensic specialists to assist with securing the network environment and investigating the extent of any unauthorized activity. The investigation, which concluded on

March 15, 2023, determined an unauthorized third party may have had access to certain during this incident.

On May 4, 2023, all impacted individuals were provided notice of the incident as well as complimentary credit monitoring and identity theft protection.

Notably, McPherson is not aware of any evidence that personal information has been misused. McPherson has not received any reports of related identity theft since the date of the incident (July 12, 2022 to present).

Number of New Hampshire Residents Affected

A total of 2 residents of New Hampshire have been identified as potentially affected by this security incident. Notification letters to these individuals will be mailed on May 4, 2023, by first class mail. A sample copy of the notification letter is attached.

Steps Taken

Upon detecting this incident, McPherson moved quickly to initiate a response, which included conducting an investigation with the assistance of IT specialists and confirming the security of the network environment. McPherson wiped and rebuilt affected systems and have taken steps to bolster network security. McPherson also reviewed and altered policies, procedures, and network security software relating to the security of systems and servers, as well as how McPherson stores and manages data.

McPherson offered free credit monitoring services to all potentially affected individuals.

Contact Information

McPherson 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

Sincerely,

Ross M. Molina of
LEWIS BRISBOIS BISGAARD & SMITH LLP

McPherson Hospital
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



Via First-Class Mail

May 4, 2023

Notice of Data Security Incident

Dear [REDACTED],

You are receiving this letter because you are a current or former patient of McPherson Hospital in McPherson, Kansas. We are writing to inform you of an incident that may have exposed your personal information. McPherson Hospital takes the privacy of personal information seriously and wants to provide you with information and resources you can use to protect your information.

What Happened:

On July 12, 2022, McPherson Hospital was the victim of a ransomware incident, in which an unauthorized third party accessed and disabled some of our systems. Upon discovering the incident, we immediately engaged third-party forensic specialists to assist us with securing the network environment and investigating the extent of any unauthorized activity. Our investigation, which concluded on March 15, 2023, determined an unauthorized third party may have acquired certain individual personal and health information during this incident.

As of this writing, McPherson Hospital has not received any reports of misuse of information and/or related identity theft since the date the incident was discovered (July 12, 2022 to present).

What Information Was Involved:

Again, we found no evidence that your information has been specifically misused. However, the following information was potentially exposed to an unauthorized third party:

What We Are Doing:

Data security is one of our highest priorities. Upon detecting this incident we moved quickly to initiate a response, which included conducting an investigation with the assistance of IT specialists and confirming the security of our network environment. We have also reviewed and enhanced our technical safeguards to prevent a similar incident.

Additionally, we are offering you access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do:

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/mcpherson> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

We encourage you to take full advantage of this service offering. Cyberscout representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call Cyberscout at 1-833-570-3013, Monday through Friday, 8:00 am to 8:00 pm ET, excluding holidays.

McPherson Hospital values the security of the personal data that we maintain, and understand the frustration, concern, and inconvenience that this incident may have caused.

Sincerely,

Lewis Newberry
President & CEO

Additional Information

Credit Reports: 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.

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:

| | | |
|---|---|--|
| Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/ | Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html | TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze |
|---|---|--|

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax ([https://assets.equifax.com/assets/personal/Fraud Alert Request Form.pdf](https://assets.equifax.com/assets/personal/Fraud%20Alert%20Request%20Form.pdf));
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

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. The phone numbers for all three credit bureaus are at listed above.

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

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For New York residents, the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and <https://ag.ny.gov/>.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.