



Allen E. Sattler
650 Town Center Drive, Suite 1400
Costa Mesa, California 92626
Allen.Sattler@lewisbrisbois.com
Direct: 714.668.5572

March 25, 2022

VIA EMAIL

Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: **Notification of Data Security Incident**

Dear Maryland Office of the Attorney General:

Lewis Brisbois Bisgaard & Smith LLP represents Super Care, Inc. dba SuperCare Health ("SuperCare") in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland's data breach notification statute, Md. Code Ann. Comm. Law §§ 14-3501-3508.

1. Nature of the data security incident.

On July 27, 2021, SuperCare experienced anomalies within its computer network. When its IT department began troubleshooting to identify and fix the issue, it learned of the presence of an unauthorized party on certain systems within its network. Upon this discovery, SuperCare immediately began containment, mitigation, and remediation measures to reduce the impact on its operations. In addition, SuperCare engaged cybersecurity experts to supplement its response efforts, including conducting a forensic investigation to identify the source of the compromise, impact on its systems and data, and the scope of any data access or exfiltration.

The forensic investigation determined that an unauthorized party gained access to SuperCare's environment and exploited a vulnerability within Microsoft's print spooler service to escalate privileges. The unauthorized third party used the escalated privileges in order to move laterally throughout the environment. The forensic investigation found that the unauthorized third party had access to its environment from July 23, 2021 to July 27, 2021. Finally, the forensic investigation revealed evidence to indicate that the unauthorized third party responsible for the incident had access to and obtained certain files maintained in SuperCare's digital environment. To date, there is no evidence to suggest that the information involved was sold, published, or otherwise misused.

SuperCare worked diligently to review the affected files and determine whether they contained personal information ("PI") or HIPAA-protected health information ("PHI"). On February 4, 2022, SuperCare determined that the potentially impacted files contained PI and PHI relating to its patients.

Concurrently, SuperCare confirmed that the initial attack vector was addressed as part of its containment, mitigation, and remediation measures, and SuperCare implemented additional safeguards to harden SuperCare's digital environment against potential future threats.

2. Number of Maryland Residents Affected

The information involved varies depending on the individual but may include the following for affected Maryland residents: name, address date of birth, patient account number, claim information, health insurance policy/member number diagnosis information and treatment information. Please note that Social Security number was involved for only 5 residents. This represents a small subset of the 43 total Maryland residents whose PI/PHI was involved in the incident. Again, SuperCare has no reason to believe that any information in the files has been or will be misused, or otherwise will be made available publicly.

3. Notification to Affected Individuals

On March 25, 2022, notification letters were sent to affected individuals via USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information. If an individual's Social Security number, driver's license number, or state identification card number was involved, the notification letter also offers complimentary identity protection services, including credit monitoring, dark web monitoring, \$1 million identity fraud loss reimbursement policy, and fully-managed identity theft recovery services. A sample notification letter is enclosed.

On the same day, SuperCare provided the enclosed media notice to media outlets in regions with 500 or more affected individuals. It also published the enclosed notice of the incident on its website. The notice will remain on the website for 90 days.

3. Steps taken relating to the incident.

Once SuperCare discovered the cause of the initial anomalies, it took immediate steps to contain the threat and recover the data to mitigate the impact of the incident to its operations. As a part of this process, SuperCare deployed a new managed endpoint detection and response ("EDR") agents on systems throughout its network to monitor such systems for any further potential threats and malicious activity. The EDR tool as well as firewall and systems logs confirmed that there are no indications of any continued access, persistence, other malicious activity, or further compromise of our systems or network.

Furthermore, SuperCare has implemented additional security measures to reduce the likelihood of a future incident. They are as follows:

- Replaced the existing EDR solution with the new managed EDR tool on all systems;
- Deployed an enterprise print solution to bypass the need for Windows print servers;
- Conducted penetration testing and a security risk assessment to identify vulnerabilities and addressed results;
- Adopted a cloud-based identity and access management system and physical authentication token to replace soft authentication token for multi-factor authentication;
- Increased network segmentation and implemented further restrictions on access to corporate services and resources; and
- Updated end user cybersecurity awareness training.

Lastly, SuperCare has reported the incident to the Federal Bureau of Investigation and is committed to assisting the FBI and any other law enforcement agencies in identifying and prosecuting those responsible for the incident.

4. Contact information.

If you have questions or concerns regarding any of the above, please do not hesitate to contact me at allen.sattler@lewisbrisbois.com or 714.668.5572. Jennifer Lee is also available to address any questions or concerns you may have, and she may be reached at jennifer.lee@lewisbrisbois.com and 714.668.5568.

SuperCare takes the privacy and security of patient information very seriously and is committed to minimizing the impact of this incident on its patients.

Very truly yours,

Allen E. Sattler of
LEWIS BRISBOIS BISGAARD & SMITH LLP

AES: JL

Encl.: Sample Notification Letters
Media Notice
Website Notice

TO ENROLL, PLEASE CALL:
1-833-648-2050
OR VISIT:
<https://response.idx.us/supercare>
Enrollment Code: <<Enrollment>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

March 25, 2022

RE: <<Variable1>>

Dear <<First Name>> <<Last Name>>,

SuperCare Health is disappointed to be among the hundreds of healthcare-related entities that have experienced a data security incident in recent years. We are writing to inform you of this data security incident as it involved your <<Variable2>>. Please read this letter carefully as it contains information about the incident, our response efforts, the type of information involved, and steps you can take to help protect your personal information.

What Happened: On July 27, 2021, we discovered unauthorized activity on our systems. In response, we immediately began containment, mitigation, and restoration efforts to terminate the activity and to secure our network, systems, and data. In addition, we retained independent cybersecurity experts to conduct a forensic investigation into the incident and assist us in determining what happened.

The forensic investigation revealed that an unknown party had access to certain systems on our network from July 23, 2021 to July 27, 2021. Based on that information, we worked diligently to identify the potentially affected files and their contents. On February 4, 2022, we determined that the potentially impacted files contained some of your information. As of the date of this letter, **we have no reason to believe your information was published, shared, or misused** as a result of this incident. Nevertheless, we are notifying you of the incident and providing you with helpful resources.

What Information Was Involved: The data involved may include: <<Variable3>>.

What We Are Doing: In addition to the response efforts as described above, we implemented additional security measures to protect our digital environment and minimize the likelihood of future incidents. We also reported the incident to the Federal Bureau of Investigation and will cooperate to help identify and prosecute those responsible.

In addition, we are offering you <<12/24>> months of free identity theft protection services through IDX, a data breach and identity recovery services expert. The identity protection services include credit monitoring, dark web monitoring, \$1 million identity theft reimbursement insurance, and fully managed identity recovery services at no cost to you. To receive these services, you must be over the age of 18 and have a Social Security number, an established credit file, and a residential address in the United States that is associated with your credit file.

What You Can Do: You can enroll in the free identity protection services offered in this letter by calling 1-833-648-2050 or visiting <https://response.idx.us/supercare> and using the Enrollment Code provided at the top of

this letter. Please note that the deadline to enroll is **June 25, 2022**. You can also review the enclosed sheet that provides additional information.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the identity protection services offered, please call 1-833-648-2050, Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time.

The privacy and security of patient information is a top priority for SuperCare Health. We take this incident very seriously and we regret any worry or inconvenience this may cause you.

Sincerely,

SuperCare Health

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
www.consumer.ftc.gov and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet & Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
www.ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
www.oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete

inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.


SuperCareHealth
Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728




CIVIL LITIGATION DIVISION
RECEIVED
APR 08 2022
Office of the Attorney General


March 25, 2022

RE: Notice of Data Breach

Dear 

SuperCare Health is disappointed to be among the hundreds of healthcare-related entities that have experienced a data security incident in recent years. We are writing to inform you of this data security incident as it involved your personal and protected health information. Please read this letter carefully as it contains information about the incident, our response efforts, the type of information involved, and steps you can take to help protect your personal information.

What Happened: On July 27, 2021, we discovered unauthorized activity on our systems. In response, we immediately began containment, mitigation, and restoration efforts to terminate the activity and to secure our network, systems, and data. In addition, we retained independent cybersecurity experts to conduct a forensic investigation into the incident and assist us in determining what happened.

The forensic investigation revealed that an unknown party had access to certain systems on our network from July 23, 2021 to July 27, 2021. Based on that information, we worked diligently to identify the potentially affected files and their contents. On February 4, 2022, we determined that the potentially impacted files contained some of your information. As of the date of this letter, we have no reason to believe your information was published, shared, or misused as a result of this incident. Nevertheless, we are notifying you of the incident and providing you with helpful resources.

What Information Was Involved: The data involved may include: name, address, date of birth, patient account number, diagnostic information, and claim information. **Your Social Security number, driver's license number, and state identification card number were NOT impacted by this incident.**

What We Are Doing: In addition to the response efforts as described above, we implemented additional security measures to protect our digital environment and minimize the likelihood of future incidents. We also reported the incident to the Federal Bureau of Investigation and will cooperate to help identify and prosecute those responsible.

What You Can Do: As noted above, we are not aware of any misuse of your information as a result of this incident. However, we encourage you to follow the recommendations on the next page.

For More Information: If you have any questions regarding the incident, please call 1-833-648-2050, Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time.

Super Care, Inc. dba SuperCare Health
8345 Firestone Blvd, Suite 210, Downey, CA 90241



The privacy and security of patient information is a top priority for SuperCare Health. We take this incident very seriously and we regret any worry or inconvenience this may cause you.

Sincerely,

SuperCare Health

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
www.consumer.ftc.gov and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet & Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
www.ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
www.oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete

inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.