



RECEIVED

MAR 25 2021

CONSUMER PROTECTION DIVISION

March 19, 2021

Michael E. Kar, Esq.
212.915.5535 (direct)
Michael.Kar@WilsonElser.com

First Class Mail

Office of the Attorney General, State of Idaho
700 W. Jefferson Street, Suite 210
P.O. Box 83720
Boise, Idaho 83720-0010

Re: Our Client : The SurgiCare Center of Utah
Matter : Data Security Incident on December 21, 2020
Wilson Elser File # : 16516.01288

Dear Attorney General Wasden:

We represent The SurgiCare Center of Utah (“SCU”) located in Salt Lake City, Utah, with respect to a potential data security incident described in more detail below. SCU 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 breach, what information has been compromised, and the steps that SCU is taking to secure the integrity of its systems. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

SCU is an eye surgical center associated with The Eye Institute of Utah, an eye care clinic located in Salt Lake City, Utah. On December 21, 2020, SCU detected that it was the target of a cybersecurity attack. An unauthorized third party attempted to infiltrate SCU’s computer network, encrypt SCU’s data, and then demand a ransom payment in exchange for decryption. Through this compromise, it is possible that certain individuals’ full name, mailing address, social security number, electronic health record data, and other medical information was exposed to cybercriminals.

2. Number of Idaho Residents Affected

A total of one hundred and eighty-eight (188) Idaho residents were potentially affected by this security incident. Notification letters to these individuals were mailed on March 16, 2021 and March 19, 2021, by first class mail. A sample copy of the notification letter is included with this letter.

150 East 42nd Street • New York, NY 10017 • p 212.490.3000 • f 212.490.3038

Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Indiana • Kentucky
Los Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • New Jersey • New Orleans • New York • Orlando • Philadelphia • Phoenix • San Diego
San Francisco • Sarasota • Stamford • Virginia • Washington, DC • West Palm Beach • White Plains

wilsonelser.com

3. Steps Taken

Upon detecting this incident, SCU moved quickly to initiate a response, which included conducting an investigation with the assistance of IT specialists and confirming the security of its network environment. SCU has reviewed and altered its policies and procedures relating to the security of its systems and servers, as well as its information life cycle management. SCU is also working with law enforcement in response to this incident.

SCU values the safety of its patients and employees' personal information and is therefore offering free identity monitoring services through Kroll. Kroll's services include: at least 12 months of credit monitoring, fraud consultation, and identity theft restoration. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. With this protection, Kroll will help the affected individuals resolve issues if their identity is compromised. Consumer contact information for Kroll is included in the attached notification letter.

4. Contact Information

SCU 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 Michael.Kar@WilsonElser.com or 212.915.5535.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Michael E. Kar, Esq.
MEK/sjb

Copy: Robert Walker, Esq. (Wilson Elser LLP), Sean Bowen, Esq. (Wilson Elser LLP)

Enclosure: *Sample Notification Letter*



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

The SurgiCare Center of Utah (“SCU”) is an eye surgical center associated with The Eye Institute of Utah (“EIU”), an eye care clinic, located in Salt Lake City, Utah. We are writing in order to inform you of an incident that may have exposed some of your sensitive personal information. We take the security of your personal information seriously and want to provide you with information and resources you can use to help protect your information.

What Happened and What Information was Involved:

On December 21, 2020, SCU detected that it was the target of a ransomware attack. An unauthorized third party infiltrated SCU’s computer network, encrypted SCU’s files, and demanded a ransom payment.

It is possible that the following information, if maintained by SCU, could have been exposed to the unauthorized third party: first and last name, mailing address, date of birth, Social Security number, electronic health record data, and other medical information.

As of this writing, SCU has not received any reports of related identity theft since the date the incident was discovered (December 21, 2020).

What We Are Doing:

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 reviewed and altered our policies and procedures relating to the security of our systems and servers, as well as our information life cycle management.

We value the safety of your personal information and are therefore offering identity monitoring services through Kroll for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

What You Can Do:

We encourage you to activate the free identity monitoring services being offered.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services. *You have until **June 17, 2021** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering.

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 1-855-515-1653, Monday through Friday, 7:00am – 4:30pm Mountain Time.

SCU values the security of the personal data that we protect, and we apologize for any inconvenience that this incident has caused.

Sincerely,

A handwritten signature in black ink, appearing to read 'D. Benson', with a long horizontal flourish extending to the right.

Drew Benson
Chief Administrative Officer

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);
- 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 the bottom of this page.

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.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.