



David McMillan, Partner
Cybersecurity & Data Privacy Team
175 Pearl Street, Suite C-402
Brooklyn, New York 11201
dmcmillan@constangy.com
Direct: 718.614.8371

April 5, 2024

VIA EMAIL

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: ldtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete LLP (“Constangy”) represents Island Ambulatory Surgery Center, LLC (“IASC”) in connection with a recent data security incident described in greater detail below.

1. Nature of the security incident.

On or around July 31, 2023, IASC became aware of unusual activity that disrupted access to certain systems. Upon discovering this activity, IASC immediately took steps to secure its network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened. Based on that investigation, IASC learned that an unauthorized actor accessed and acquired certain files stored in its network, some of which contained personal and / or protected health information. Following a comprehensive review of the affected files, on February 7, 2024, IASC confirmed that personal information belonging to certain Maryland residents may have been involved. IASC then took steps to notify those individuals as quickly as possible.

2. Number of Maryland residents affected.

IASC notified ten (10) Maryland residents of this incident via first class U.S. mail on April 5, 2024. The information potentially impacted in connection with this incident varies by individual but may include name, date of birth, Social Security number, driver’s license number, medical information and / or health insurance information.

A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as IASC discovered this incident, IASC took steps to secure its network environment and launched an investigation to determine what happened and the scope of personal and protected health information potentially impacted. In addition, IASC implemented measures to enhance the security

April 5, 2024

Page 2

of its environment in an effort to minimize the risk of a similar incident occurring in the future. IASC also notified the Federal Bureau of Investigation.

IASC has established a toll-free call center through IDX, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. In addition, while IASC is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, IASC is also providing complimentary credit and identity protection services to notified individuals whose Social Security numbers may have been impacted.

4. Contact information.

IASC remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Constangy.

Best regards,

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

David McMillan
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Sample Notification Letter


ISLAND AMBULATORY
SURGERY CENTER
Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

April 5, 2024

Subject: Notice of Data <<Variable Text 1 – Breach or Security Incident>>:

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a data security incident experienced by Island Ambulatory Surgery Center, LLC (“IASC”) that may have affected your personal information. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Happened: On or around July 31, 2023, IASC became aware of unusual activity that disrupted access to certain systems. Upon discovering this activity, we immediately took steps to secure our network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened. Based on that investigation, we learned that an unauthorized actor accessed and acquired certain files stored in our network, some of which contained personal information. On February 7, 2024 we determined that your information may have been impacted, and moved as quickly as possible to provide notice and resources to assist.

What Information Was Involved: The information involved in this incident may have included your name as well as your <<Variable Text – Impacted personal information categories>>.

What We Are Doing: As soon as we discovered this incident, we took immediate steps to secure our environment and enlisted a leading, independent cybersecurity firm to conduct a forensic investigation. We also reported the incident to the FBI and will cooperate with any resulting investigation. In addition, we have implemented several measures to enhance our network security and reduce the risk of similar future incidents.

We are also providing you with the opportunity to enroll in complimentary credit monitoring and identity theft protection services through IDX – a data breach and recovery services expert. These services include: <<12 months/24 months>> of credit¹ and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. Please note that the deadline to enroll is July 5, 2024.

What You Can Do: We encourage you to enroll in the credit monitoring and identity protection services we are offering, which are at no cost to you. Please also review the guidance at the end of this letter which includes additional resources you may use to help protect your information.

¹To receive credit monitoring 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.

For More Information: IASC has engaged a special call center to help answer your questions about the incident and services being offered. Representatives are available through July 5, 2024 to assist you with questions regarding this incident, between the hours of 9:00 a.m. to 9:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please visit <https://app.idx.us/account-creation/protect> or call the call center toll-free at 1-888-593-7768 or scan the QR code and provide the representative with your enrollment code listed above to enroll.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'K. Gayle', followed by a long horizontal line extending to the right.

Karlene Gayle, MSN-Ed, BSN, RN
Administrator/DON
Island Ambulatory Surgery Center, LLC
2279-83 Coney Island Avenue
Brooklyn, NY 11223

STEPS YOU CAN TAKE TO HELP PROTECT YOUR 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 <http://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 <http://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
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

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

New York Attorney General

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

North Carolina Attorney General

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

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
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>.