



Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

December 30, 2020

VIA ELECTRONIC SUBMISSION

Attorney General Aaron Frey
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 Attorney General Frey:

We represent South Country Health Alliance (“SCHA”) with respect to a recent data security incident described in greater detail below. SCHA is taking steps to prevent similar incidents from occurring in the future.

1. Nature of the security incident.

On September 14, 2020, SCHA discovered that unauthorized access to an employee email account occurred on June 25, 2020. SCHA immediately secured the account, began an investigation, and engaged cybersecurity experts to assist with the investigation. On November 5, 2020, following a review of the contents of the email account, SCHA determined that personal information belonging to some SCHA current and former employees and patients may have been in the account. In response, SCHA took steps to identify current mailing addresses for the potentially impacted individuals so that SCHA could complete notification.

2. Number of Maine residents affected.

SCHA notified three (3) residents of Maine of this data security incident via first class U.S. mail on December 30, 2020. A sample copy of the notification letter sent to the affected individuals is included with this correspondence.

3. Steps taken relating to the incident.

SCHA has taken steps in response to this incident to strengthen the security of personal information in its possession, in an effort to prevent similar incidents from occurring in the future. These steps include enhancing the security of our email environment, enhancing password protections, adopting multifactor authentication and enhancing employee security training. In addition, although SCHA is not aware of any misuse of personal information, SCHA has offered affected individuals 12 months of credit monitoring and identity remediation services through IDX.

4. Contact information.

SCHA 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 me at (214) 722-7141 or by e-mail at lindsay.nickle@lewisbrisbois.com.

Please let me know if you have any questions.

Respectfully,



Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

LBN

Encl. Copy of Consumer Notification Letter

cc: Jacqueline Leahy, Associate, Lewis Brisbois Bisgaard & Smith LLP

SOUTH COUNTRY HEALTH ALLIANCE

C/O IDX
PO Box 4129
Everett WA 98204

ENDORSE



NAME

ADDRESS1

ADDRESS2

CSZ

COUNTRY



SEQ
CODE 2D
Ver 1A

BREAK

To Enroll, Please Call:
1-833-920-3172
Or Visit:
<https://response.idx.us/schaprotect>
Enrollment Code: <<XXXXXXXXXX>>

December 30, 2020

Re: Notice of Data Breach

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

We are writing to inform you of a data security incident that may have affected your personal information. South Country Health Alliance takes the privacy and security of your personal information very seriously. We are sending you this letter to notify you about this incident, offer you credit and identity monitoring services, and inform you about steps you can take to protect your personal information.

What Happened. On September 14, 2020, we discovered that unauthorized access to an employee email account had occurred on June 25, 2020. South Country Health Alliance immediately secured the account, began an investigation, and engaged cybersecurity experts to assist us with the investigation. On November 5, 2020, following a review of the contents of the email account, we determined that your personal information may have been in the account. In response to learning this, we took steps to identify mailing addresses for potentially impacted individuals, and now we are notifying you about the incident and are providing information to assist you.

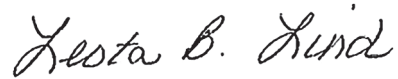
What Information Was Involved. The following information may have been involved: <<DATA SETS>>.

What We Are Doing. As soon as we discovered the incident, we took the steps referenced above. We also enhanced the security of our email environment, enhanced password protections, adopted multifactor authentication and enhanced employee security training. Additionally, we are offering 12 months of credit monitoring and identity protection services at no cost to you and providing you additional information about steps you can take to protect your personal information.

What You Can Do. You can follow the recommendations on the following page to protect your personal information. In addition, we encourage you to enroll in the identity theft protection services we are offering through IDX. The identity protection services include 12 months of credit and CyberScan monitoring, a \$1,000,000 identify theft insurance policy, and fully managed identity theft recovery services. To 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. You can enroll in the free IDX identity protection services by calling 1-833-920-3172 or going to <https://response.idx.us/schaprotect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. Please note the deadline to enroll is March 30, 2021.

For More Information. If you have questions or need assistance, please call 1-833-920-3172, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time, or visit <https://response.idx.us/schaprotect>. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in cursive script that reads "Leota B. Lind".

Leota Lind
Chief Executive Officer
South Country Health Alliance

Steps You Can Take to Further 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 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 can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion P.O. Box 1000 Chester, PA19016 1-800-909-8872 www.transunion.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-685-1111 www.equifax.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 www.annualcreditreport.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 90 days. 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: Under U.S. law, 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.

Minnesota Residents: A report discussing the facts of this incident and the results of the investigation has been prepared and will be made available to you upon request. If you would like a copy of the report, please call 1-833-920-3172 and tell the call center representative that you would like a copy of the report. In order for us to fulfill your request, you will be required to provide a mailing address or an email address to the call center representative.

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. Contact information for the FTC is: **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov and www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

New York Attorney General Bureau of Internet and Technology Resources 28 Liberty Street New York, NY 10005 ifraud@ag.ny.gov 1-212-416-8433	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 www.oag.state.md.us 1-888-743-0023	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 401-274-4400
---	---	---	---

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 others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf

