



Laura K. Funk
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Laura.Funk@lewisbrisbois.com
Direct: 972.942.5696

July 5, 2022

VIA EMAIL

Attorney General Brian Frosh
Maryland Attorney General's Office
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
E-Mail: ldtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Frosh:

We represent Southwest Health Center ("Southwest Health"), a nonprofit community healthcare provider headquartered in Platteville, Wisconsin. This letter is being submitted because the personal information of eleven (11) Maryland residents may have been involved in a recent data security incident experienced by Southwest Health. The incident may have involved unauthorized access to, and acquisition of, the name and Social Security number, clinical or treatment information, health insurance information, and/or date of birth of these individuals.

On January 11, 2022, Southwest Health detected unusual activity in its network environment. Upon discovering this activity, Southwest Health took steps to secure its network and launched an investigation with the assistance of a leading, independent forensics firm engaged to determine what happened and whether sensitive information was accessed or acquired without authorization during the course of the incident. As a result of the investigation, Southwest Health learned that certain of its folders had been accessed and acquired without authorization. Southwest Health then retained experts to conduct a comprehensive review of the contents of those files, which was completed on May 27, 2022, and determined that the impacted systems contained personal information belonging to certain individuals. Southwest Health then worked diligently to identify current address information required to provide notification.

In response to the incident, Southwest Health notified the Federal Bureau of Investigation and has cooperated with law enforcement efforts. Further, Southwest Health notified potentially affected residents in your State of this incident via U.S. First-Class Mail on July 5, 2022, a sample letter of which is attached. In so doing, Southwest Health offered 12 months of complimentary credit monitoring and identity theft restoration services through IDX. These services include Credit Monitoring, Identity Restoration, and \$1 Million Identity Theft Insurance.

July 5, 2022
Page 2

Please do not hesitate to contact me should you have any questions.

Best regards,

A handwritten signature in cursive script, reading "Laura K. Funk".

Laura K. Funk of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Adult & Minor Consumer Notification Letter



Southwest
—HEALTH—

P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:

1-833-423-2983

Or Visit:

<https://response.idx.us/southwesthealth>

Enrollment Code: [XXXXXXXXXX]

<<First Name>> <<Last Name>>

<<Address1>> <<Address2>>

<<City>>, <<State>> <<Zip>>

July 5, 2022

Re: Notice of Data <<Security Incident / Breach>>

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

We are writing to inform you of a recent data security incident that may have involved some of your personal information. At Southwest Health Center ("Southwest Health"), we are committed to the privacy and security of all personal information in our possession. This is why we are writing to notify you of this incident, to offer you complimentary identity monitoring services, and to inform you about steps you can take to help safeguard your personal information.

What Happened? On January 11, 2022, Southwest Health discovered a potential data security incident affecting certain systems. Upon discovering this, we immediately took steps to secure our network and launched an investigation with the assistance of cybersecurity experts to determine what happened and whether sensitive information may have been affected. The investigation subsequently revealed that certain personal information may have been accessed or acquired without authorization. We then initiated a comprehensive review of the data to determine the types of information involved and to identify the potentially impacted individuals. Following completion of the data review, we then worked diligently to gather current contact information needed to notify all potentially affected individuals. This process was completed on May 27, 2022.

What Information Was Involved? The information may have involved your name and your <<variable>>.

What We Are Doing. As soon as we discovered this incident, we took the measures referenced above and implemented enhanced security measures to help prevent a similar incident from occurring in the future. We also notified the Federal Bureau of Investigation and were informed that data servers involved in the incident had been identified and confiscated. However, out of an abundance of caution, we are providing you information about steps you can take to help protect your personal information and identity protection services through IDX, a data security and recovery services expert. Your complimentary enrollment in IDX identity protection includes <<12/24 months>> of: credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. Additional information about these services is included with this letter.

What You Can Do. Please follow the recommendations included with this letter to help protect your personal information. You can also enroll in the IDX identity protection services being provided to you, at no cost, through IDX. To enroll, please visit the IDX website at <https://response.idx.us/southwesthealth> and provide your enrollment code located at the top of this page. Please note that the deadline to enroll is October 5, 2022. Additional information describing the IDX identity protection services is included with this letter.

For More Information. If you have any questions or need assistance, please call 1-833-423-2983 Monday through Friday from 8:00 am to 8:00 pm Central Time. Our representatives are fully versed on this incident and can answer any questions you may have regarding how to help safeguard your personal information.

Thank you for your patience through this incident. We take your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,
Jesse Sookchoff
Chief Administrative & Financial Officer
Southwest Health Center

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 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:

TransUnion

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

Experian

P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

Equifax

P.O. Box 740241
Atlanta, GA 30374
1-866-349-5191
www.equifax.com

Free Annual Report

P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about 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
https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf
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 [http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf](https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf).



Enrollment in IDX Identity Protection

Website and Enrollment. Please visit <https://response.idx.us/southwesthealth> and follow the instructions for enrollment using your Enrollment Code included with this letter.

Activate the credit monitoring provided as part of your IDX membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at **1-833-423-2983** to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

This IDX enrollment will include one-year enrollment into:

SINGLE BUREAU CREDIT MONITORING - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCAN™ - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY - IDX fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDX Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.



P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:

1-833-423-2983

Or Visit:

<https://response.idx.us/southwesthealth>

Enrollment Code: [XXXXXXXXXX]

To The Parent or Guardian of

<<First Name>> <<Last Name>>

<<Address1>> <<Address2>>

<<City>>, <<State>> <<Zip>>

July 5, 2022

Re: Notice of Data <<Security Incident / Breach>>

Dear Parent or Guardian of <<First Name>> <<Last Name>>,

We are writing to inform you of a recent data security incident that may have involved some of your child's personal information. At Southwest Health Center ("Southwest Health"), we are committed to the privacy and security of all personal information in our possession. This is why we are writing to notify you of this incident, to offer you complimentary identity monitoring services, and to inform you about steps that can be taken to help safeguard your child's personal information.

What Happened? On January 11, 2022, Southwest Health discovered a potential data security incident affecting certain systems. Upon discovering this, we immediately took steps to secure our network and launched an investigation with the assistance of cybersecurity experts to determine what happened and whether sensitive information may have been affected. The investigation subsequently revealed that certain protected health information may have been accessed or acquired without authorization. We then initiated a comprehensive review of the potentially impacted data to determine the types of personal information involved and identify the potentially impacted individuals. Following completion of the data review, we then worked diligently to gather current contact information needed to notify all potentially affected individuals. This process was completed on May 27, 2022.

What Information Was Involved? The information may have involved your child's name and their <<variable>>.

What We Are Doing. As soon as we discovered this incident, we took the measures referenced above and implemented enhanced security measures to help prevent a similar incident from occurring in the future. We also notified the Federal Bureau of Investigation and were informed that data servers involved in the incident had been identified and confiscated. However, out of an abundance of caution, we are providing you information about steps you can take to help protect your child's personal information and identity protection services through IDX, a data security and recovery services expert. Your complimentary enrollment in IDX identity protection includes <<12/24 months>> of: CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. Additional information about these services is included with this letter.

What You Can Do. Please follow the recommendations included with this letter to help protect your child's personal information. You can also enroll in the IDX identity protection services being provided to you, at no cost, through IDX. To enroll, please visit the IDX website at <https://response.idx.us/southwesthealth> and provide the enrollment code located at the top of this page. Please note that the deadline to enroll is October 5, 2022. Additional information describing the IDX identity protection services is included with this letter.

For More Information. If you have any questions or need assistance, please call 1-833-423-2983 Monday through Friday from 8:00 am to 8:00 pm Central Time. Our representatives are fully versed on this incident and can answer any questions you may have regarding how to help safeguard your child's personal information.

Thank you for your patience through this incident. We take your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Jesse Sookochoff
Chief Administrative & Financial Officer
Southwest Health Center

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 child's account statements 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).

Personal Information of a Minor: You can request that each of the three national consumer reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the consumer reporting agency. You can also report any misuse of a minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>. Contact information for the three national credit reporting agencies is below.

Security Freeze: You may place a free credit freeze for minors under age 16. By placing a security freeze, someone who fraudulently acquires the minor's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the 3 national credit reporting bureaus listed below to place the freeze. Keep in mind that when you place the freeze, the minor will not be able to borrow money, obtain instant credit, or get a new credit card until the freeze is temporarily lifted or permanently removed. You must separately place a security freeze on the minor's credit file with each credit reporting agency. There is no charge to place, lift, or remove a security freeze on the minor's credit files. In order to place a security freeze, you may be required to provide the credit reporting agency with information that identifies you and/or the minor, including birth or adoption certificate, Social Security card, and government issued identification card.

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 the minor's credit report. An initial fraud alert is free and will stay on the minor's credit file for at least one year. The alert informs creditors of possible fraudulent activity within the minor's report and requests that the creditor contact you prior to establishing any accounts in the minor's name. To place a fraud alert on the minor's credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

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
identitytheft.gov
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 the minor's 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>.



Enrollment in IDX Identity Protection

Website and Enrollment. Please visit <https://response.idx.us/southwesthealth> and follow the instructions for enrollment using your Enrollment Code included with this letter.

Telephone. Contact IDX at **1-833-423-2983** to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

This IDX enrollment will include one-year enrollment into:

CYBERSCAN™ - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY - IDX fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDX Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.