



Allen Sattler, Partner & Vice-Chair
Cybersecurity & Data Privacy Team
Plaza Tower
600 Anton Blvd, 11th Floor
Costa Mesa, California 92626
asattler@constangy.com
315.430.4888

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

August 1, 2023

VIA ONLINE PORTAL

Attorney General Aaron Frey
Maine Attorney General's Office
Consumer Protection Division
6 State House Station
Augusta, ME 04333
Email: attorney.general@maine.gov

Re: Notice of Data Security Incident

Dear Attorney General Frey:

Constangy, Brooks, Smith & Prophete, LLP represents MHMR Authority of Brazos Valley ("MHMR"), a non-profit healthcare organization based out of Texas, 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 Maine's data breach notification statute.

Nature of the Security Incident

On November 5, 2022, MHMR experienced a security incident disrupting access to certain of its computer systems. In response, MHMR immediately took steps to secure its digital environment and engaged a leading cybersecurity firm to assist with an investigation and determine whether sensitive or personal information may have been accessed or acquired during the incident. As a result of the investigation, MHMR identified that certain data may have been accessed or acquired without authorization. MHMR then engaged an independent vendor to conduct a comprehensive review of all potentially affected data, and on May 30, 2023, MHMR determined that the personal and protected health information of individuals, including certain employees and patients that received services from MHMR, may have been affected. MHMR then exhausted its resources to diligently obtain and compile missing address information, where available, to effectuate notification to those potentially affected, which was completed on July 17, 2023.

The information affected varied between individuals but may have included name, Social Security number, driver's license number, medical record number, Medicaid or Medicare number, medical treatment and/or diagnosis information, and/or health insurance information. Please know that at this time, we have no knowledge that personal or protected health information was used to commit identity theft or for other illicit financial gain. However, out of an abundance of caution, MHMR has worked to identify all potentially affected individuals in order to provide notice of the incident.

Alabama Arkansas California Colorado District of Columbia Florida Georgia Illinois
Indiana Maryland Massachusetts Minnesota Missouri New Jersey New York
North Carolina Oregon Pennsylvania South Carolina Tennessee Texas Virginia Washington

Number of Maine Residents Involved

On July 28, 2023, MHMR notified eight (8) Maine residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

Steps Taken to Address the Incident

In response to the incident, MHMR is providing individuals with information about steps that they can take to help protect their personal information, and, out of an abundance of caution, it is also offering those with certain personal information impacted complimentary credit monitoring and identity protection services through IDX. Additionally, to help reduce the risk of a similar future incident, MHMR has implemented additional technical security measures throughout the environment.

Contact Information

MHMR remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at ASattler@Constangy.com.

Sincerely,



Allen Sattler
Partner & Vice-Chair, Cybersecurity & Data Privacy Team

Encl:
Sample Consumer Notification Letter



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

To Enroll, Please Call:
1-888-220-4956
Or Visit:
<https://response.idx.us/MHMR>
Enrollment Code: <<Enrollment Code>>

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

July 28, 2023

Re: Notice of Data <<Variable Text 1>>

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

I am writing to inform you of a data security incident experienced by MHMR Authority of Brazos Valley (“MHMR”) that may have affected your personal information. MHMR takes the privacy and security of all personal information, including protected health information, within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened? On November 5, 2022, we experienced a security incident disrupting access to certain of our computer systems. In response, we took immediate steps to secure our systems and promptly launched an investigation. In so doing, we engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result, including the engagement of an independent team to perform a comprehensive review of all data that may have been affected by the incident. On or about May 30, 2023, this review identified that the personal and/or protected health information related to certain MHMR employees and patients may have been involved. MHMR then exhausted its resources to diligently obtain and compile missing address information, where available, to effectuate notification to those potentially affected, which was completed on July 17, 2023.

What Information Was Involved? The information potentially impacted in connection with this incident may have included your name, <<Variable Text 2 - Data Element>>. Please know that at this time, we have no knowledge that personal information was used to commit identity theft or for other illicit financial gain. However, out of an abundance of caution, MHMR has worked to identify all potentially affected individuals in order to provide notice of the incident and recommendations you can take on how to protect your information.

What We Are Doing. As soon as MHMR discovered this incident, we took the steps described above. In addition, we implemented measures to enhance the security of our environment in an effort to minimize the risk of a similar incident occurring in the future. We also reported the incident to law enforcement and are cooperating with the FBI to aid in their investigation.

Additionally, we are offering you the opportunity to enroll in credit monitoring and identity protection services through IDX, at no cost to you. The IDX services, which are free to you upon enrollment, include <<12/24 months>> of credit monitoring and CyberScan dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you to resolve issues if your identity is compromised.

What You Can Do. Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information. In addition, we encourage you to enroll in the credit

monitoring and identity theft protection services we are offering through IDX at no cost to you. 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 IDX identity protection services by calling 1-888-220-4956 or going to <https://response.idx.us/MHMR> 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 October 28, 2023.

For More Information. If you have questions, please call IDX at 1-888-220-4956, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. IDX representatives are fully versed on this incident and can answer questions you may have regarding the protection of your personal information.

The security of your information is a top priority at MHMR and protecting employee and patient information at all costs is a critical operational piece to MHMR's role as a care provider. Please accept our sincere apologies and know that we take this matter very seriously and deeply regret any worry or inconvenience this may cause you.

Sincerely,



Ken Danford
Director Administrative Services
MHMR Authority of Brazos Valley
1504 South Texas Avenue
Bryan, TX 77802

ADDITIONAL 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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

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:

Equifax, P.O. Box 740241, Atlanta, GA 30374, 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 Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. 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>. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. 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.

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.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov

California: California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.gov/>

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; <https://www.maine.gov/ag/>

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

Oregon: Oregon Office of the Attorney General can be reached at: Oregon Department of Justice, 1162 Court St. NE, Salem, OR, 97301, 1-877-877-9392, www.doj.state.or.us

Rhode Island: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>.

Texas: Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov



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

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

July 28, 2023

Re: Notice of Data <<Variable Text 1>>

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

I am writing to inform you of a data security incident experienced by MHMR Authority of Brazos Valley (“MHMR”) that may have affected your personal information. MHMR takes the privacy and security of all personal information, including protected health information, within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened? On November 5, 2022, we experienced a security incident disrupting access to certain of our computer systems. In response, we took immediate steps to secure our systems and promptly launched an investigation. In so doing, we engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result, including the engagement of an independent team to perform a comprehensive review of all data that may have been affected by the incident. On or about May 30, 2023, this review identified that the personal and/or protected health information related to certain MHMR employees and patients may have been involved. MHMR then exhausted its resources to diligently obtain and compile missing address information, where available, to effectuate notification to those potentially affected, which was completed on July 17, 2023.

What Information Was Involved? The information potentially impacted in connection with this incident may have included your name, <<Variable Text 2 - Data Element>>. Please know that at this time, we have no knowledge that personal information was used to commit identity theft or for other illicit financial gain. However, out of an abundance of caution, MHMR has worked to identify all potentially affected individuals in order to provide notice of the incident and recommendations you can take on how to protect your information.

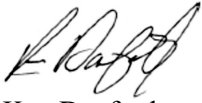
What We Are Doing. As soon as MHMR discovered this incident, we took the steps described above. In addition, we implemented measures to enhance the security of our environment in an effort to minimize the risk of a similar incident occurring in the future. We also reported the incident to law enforcement and are cooperating with the FBI to aid in their investigation.

What You Can Do. Receiving this letter does not mean that you are the victim of identity theft. We recommend, however, that you review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information.

For More Information. If you have questions, please call IDX at 1-888-220-4956, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. IDX representatives are fully versed on this incident and can answer questions you may have regarding the protection of your personal information.

The security of your information is a top priority at MHMR and protecting employee and patient information at all costs is a critical operational piece to MHMR's role as a care provider. Please accept our sincere apologies and know that we take this matter very seriously and deeply regret any worry or inconvenience this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'Ken Danford', written in a cursive style.

Ken Danford
Director Administrative Services
MHMR Authority of Brazos Valley
1504 South Texas Avenue
Bryan, TX 77802

ADDITIONAL 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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

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:

Equifax, P.O. Box 740241, Atlanta, GA 30374, 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 Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. 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>. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. 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.

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.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov

California: California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.gov/>

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; <https://www.maine.gov/ag/>

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

Oregon: Oregon Office of the Attorney General can be reached at: Oregon Department of Justice, 1162 Court St. NE, Salem, OR, 97301, 1-877-877-9392, www.doj.state.or.us

Rhode Island: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>.

Texas: Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov