

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

Jason Goodwin
jgoodwin@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

December 13, 2023

Via Email

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

RE: Data Breach Notification

To Whom It May Concern:

We serve as counsel for Magnolia Bankshares Incorporated, ("MBI") located at 130 Oak Street, Eastman, Georgia 31023. We write to provide notification of a recent data security incident. By providing this notice, MBI does not waive any rights or defenses under Maryland State law, including the data breach notification statute.

On July 17, 2023, MBI discovered potentially suspicious activity related to an employee email account. Upon discovery, MBI immediately performed a password reset and engaged a third-party forensic team to assist with the investigation. A thorough investigation ultimately revealed that one employee email account was subject to unauthorized access for a limited period of time from June 27, 2023 through July 17, 2023. While we have no reason to believe sensitive information was compromised during the period of access, a review was conducted to determine the type of information potentially at risk and to whom it relates. This review was completed on October 2, 2023, and MBI worked to confirm up to date address information to provide individuals with notice.

On December 8, 2023, MBI received its results from a National Change of Address (NCOA) search and learned that 1 potentially affected individual resides within Maryland. The information potentially impacted included first and last name, date of birth, driver's license/state issued identification number, payment card information, financial account information, and/or Social Security number.

In response to this incident, MBI conducted an investigation and changed account passwords. Additionally, MBI began providing notice to the potentially impacted individuals on December 13, 2023 via U.S. mail. A copy of the notice is attached as **Exhibit A**. In an abundance of caution, MBI is offering the potentially impacted individuals complimentary credit monitoring and identity protection services.

Very truly yours,



Jason Goodwin, Esq.

Exhibit A

Magnolia State Bank
130 Oak Street
Eastman, GA 31023
DB08236 1-1



<<Name>>
<<Address>>



December 13, 2023

Dear <<Name>>,

Magnolia State Bank writes to notify you of an incident experienced by its parent company, Magnolia Bankshares, Inc. ("MBI"), that may have involved some of your personal information as described below. We take the privacy of information in our care seriously. At this time, there is no evidence to suggest that any of your information was actually viewed or misused. In an abundance of caution, we are providing you information about the incident, our response, and steps you can take to protect your information should you feel it is necessary to do so.

What Happened? On July 17, 2023, MBI discovered potentially suspicious activity related to an employee email account. Upon discovery, we took immediate action to address and investigate the incident, including performing a password reset in an abundance of caution and engaging third-party specialists to assist in conducting a full investigation. The investigation ultimately determined that one employee email account experienced unauthorized access on June 26, 2023 and July 17, 2023. Importantly, no other bank systems were affected in relation to this incident. While there is no evidence to suggest sensitive information was viewed or misused, we then began a thorough review of the contents of the account in an abundance of caution to determine the type of information contained within the impacted mailbox and to whom that information related. On November 6, 2023, this process was completed, and we worked to confirm up-to-date address information to provide you with this notification as soon as possible.

What Information Was Involved? The information potentially impacted during the incident may have included your first and last name in combination with the following data element(s): <<Data Elements>>.

What We Are Doing. We have taken the steps necessary to address the incident and are committed to fully protecting the information that you have entrusted to us. Upon learning of this incident, we performed password resets and undertook a thorough investigation. Additionally, we are offering you complimentary credit monitoring and identity protection services.

What You Can Do. We recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft.

For More Information: Should you have any questions or concerns, please contact our dedicated assistance line at 1-833-602-3223, Monday through Friday 8 am to 8 pm ET, excluding holidays. The security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support.

Sincerely,

The MSB Team

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/magnoliabankshares> and follow the instructions provided. When prompted please provide the following unique code to receive services: **M3TZ7RJLRP**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended fraud alert on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a credit freeze on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and <https://www.marylandattorneygeneral.gov>. Magnolia Bankshares, Inc. may be contacted at 130 Oak Street, Eastman, GA 31023.

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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) 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 https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 0 Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>. Magnolia Bankshares, Inc. may be contacted at 130 Oak Street, Eastman, GA 31023.