

Brad C. Moody
T: (601) 914-6108
brad.moody@nelsonmullins.com

106 S. President St., Suite 400
Jackson, MS 39201
M: 404.322.6000 F: 404.322.6050
nelsonmullins.com

August 15, 2023

Attorney General Anthony Brown
200 St. Paul Place
Baltimore, Maryland 21202
Idtheft@oag.state.md.us

Re: Sunflower Bank, N.A. - Notice of Data Incident

Dear Attorney General Brown:

I serve as outside legal counsel to Sunflower Bank, N.A. ("Sunflower Bank" or the "Bank"), which is a regional community bank with its principal place of business at 1400 16th St., Suite 250, Denver, CO 80202.¹¹ This correspondence is to notify you that Sunflower Bank is issuing consumer notices in response to the MOVEit software zero-day.

Like thousands of other organizations, across many industries around the world, the Bank utilizes MOVEit software for securely transferring sensitive and confidential information and other data. The MOVEit software is not part of the Bank's core processing systems. Instead, the software operates with an on-premises server segmented from the Bank's other IT systems.

Upon receiving notice on May 31, 2023, from the Bank's third-party software provider, Progress Software Company, of the vulnerability in its MOVEit software, the Bank promptly enacted response protocols to address the zero-day vulnerability and protect the Bank's data. In addition, a third-party forensic expert was retained, and a comprehensive investigation was launched to determine the nature and scope of the incident.

Since receiving notice of the situation, the Bank has been in regular contact with Progress Software and has implemented all fixes to the software that Progress Software has issued. However, before Progress Software notified the Bank of the vulnerability, it is believed that an unauthorized party likely took advantage of the flaw in the MOVEit software and downloaded copies of files from the Bank's server that housed the MOVEit software. After confirming the likely scope of the incident, the Bank conducted a thorough review of the impacted data to determine whether sensitive information was present and to identify individuals whose information may have

¹¹ Sunflower Bank is a nationally chartered bank regulated by the Office of the Comptroller of the Currency and is subject to the Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801 et. seq.). By providing this notice, Sunflower Bank does not waive any rights or defenses regarding the applicability of state law, the applicability of the state's data event notification statute, or personal jurisdiction.

Attorney General Anthony Brown
August 15, 2023
Page 2

been involved. On July 14, 2023, the Bank posted a public notice of the event on the main page of its website.¹²

In an abundance of caution, notification letters will begin going out via U.S. Mail to 75 residents of your State on or about August 14, 2023. The notification letters include instructions for activating credit monitoring services at no cost to the recipients. The PII that was potentially at risk included first and last name, social security number and account number. A sample notification letter is enclosed for your reference and includes:

- A description of the security event;
- Steps taken to investigate;
- Steps taken to mitigate any potential harm to consumers;
- Instructions for activating free identity theft protection services that include credit monitoring and a \$1 million insurance reimbursement policy to all consumers who received notification;
- Instructions on how to place a security freeze on the recipient's consumer credit report; and
- Instructions regarding how to obtain more information about this event, etc.

Sunflower Bank is fully committed to protecting consumer privacy and the confidentiality of personal information. To that end, the Bank has a written information security policy. We will follow-up this correspondence with any forms or other documents that may need to be completed. Please contact me if you require any additional information regarding this incident.

Best regards,



Brad Moody

Enclosure:
Sample Notification Letter

¹² <https://www.sunflowerbank.com/homepage/notice-of-third-party-moveit-data-breach/>



Sunflower Bank
First National 1870



Guardian
Mortgage

Return Mail Processing
PO Box 999
Suwanee, GA 30024

369 1 126390 *****AUTO**5-DIGIT 88007

SAMPLE A. SAMPLE - L01

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



August 14, 2023

Re: Notice of Security Incident

Dear Sample A. Sample,

We are notifying you of a recent security incident that may have involved some of your personal information.

What happened? On or about May 31, 2023, Sunflower Bank, N.A. (the “Bank”) was notified by a third-party software provider, Progress Software Corporation, of a vulnerability in Progress Software’s MOVEit file transfer software. Like thousands of other organizations, across many industries around the world, the Bank utilizes MOVEit for securely transferring sensitive and confidential information and other data. The MOVEit software is not part of the Bank’s core processing systems. Instead, the software operates with an on-premises server that is segmented from the Bank’s other IT systems. All other systems at the Bank operate independently from the MOVEit software dedicated server and were not impacted by this matter.

Upon receiving notice from MOVEit, we promptly enacted incident response protocols, and outside technical experts were engaged to investigate. Since receiving notice of the situation, the Bank has been in regular contact with Progress Software and has implemented all fixes to the software that Progress Software has issued. We are continuing to closely monitor the system for any unusual activity. We also reported this incident to law enforcement.

What information was involved? As this incident originated from and was limited to a vulnerability within Progress Software’s MOVEit software, we worked closely with Progress Software to identify the potentially impacted files for sensitive information. Currently, we do not have any evidence that anyone has misused your information. However, we are notifying you out of an abundance of caution that the potentially impacted files, which varies by individual, may have included your first and last name, [Extra1], and other information you may have shared with the Bank in connection with any financial transactions.

What are we doing and what can you do? While we are not aware of any instances of fraud at this time, we recommend you consider taking precautions, and remain vigilant against incidents of identity theft and fraud. As a precaution, the Bank encourages you to review your account statements and to monitor your personal information for suspicious activity and to detect errors.

Also, for your peace of mind, we are offering you [12/24] months of **free** credit monitoring and \$1 million in identity theft insurance through Experian. **You must activate the Experian product by the activation date for it to be effective. The activation instructions are included with this notification.** We also have enclosed some additional steps that you can take to protect yourself as you deem appropriate.

For more information about this incident, please call 833-346-1617 between 6 a.m. to 8 p.m. PST, Monday - Friday; and between 8 a.m. to 5 p.m. PST, Saturday - Sunday (excluding major U.S. holidays).

We want you to know that we take the protection of your data seriously and encourage you to take advantage of the services offered.

Sincerely,

Sunflower Bank, N.A.



First National 1870 and Guardian Mortgage are divisions of Sunflower Bank, N.A. | NMLS# 709491

STEPS YOU CAN TAKE:

Below is information on steps you can take to protect yourself if you feel necessary.

➤ **ACTIVATE Your FREE Experian IdentityWorks Product NOW in Three Easy Steps.** To help protect your identity, we are offering you a complimentary **[12/24]-month membership** to Experian's IdentityWorks product. This product helps detect possible future misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks Alert is completely free to you and enrolling in this program will not hurt your credit score.

STEP 1 ENSURE You Enroll By: October 31, 2023 (Your code will not work after this date.)

STEP 2 VISIT the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit

STEP 3 PROVIDE Your Activation Code: ABCDEFGHI

If you have questions about the IdentityWorks or need an alternative to enrolling online, **please call 833-346-1617** and provide engagement **[Engagement Number]**. A credit card is not required for enrollment.

Once your IdentityWorks membership is activated, you will receive the following features:

- **Experian Credit Report at Signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Restoration Agents are immediately available to help address credit/non-credit related fraud.
- **\$1 Million Identity Theft Insurance:**² Provides coverage for certain costs and unauthorized electronic fund transfers.

You must activate your membership by the Enrollment Date (noted above) by enrolling at <https://www.experianidworks.com/3bcredit> or calling 833-346-1617 to register your activation code above in order for this service to be activated.

Once your enrollment in IdentityWorks is complete, carefully review your credit report for inaccurate or suspicious items. If you have any questions about IdentityWorks, need help understanding something on your credit report, or suspect that an item on your credit report may be fraudulent, please contact Experian's customer team at **833-346-1617**.

Additional Steps You May Wish to Take:

➤ **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS & REPORT FRAUD. CHANGE PASSWORDS AND SECURITY VERIFICATION QUESTIONS & ANSWERS.** Carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity, changing passwords/security verifications as needed – particularly if same password is used over multiple online accounts.

➤ **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 877-322-8228 to obtain one free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify any accounts you did not open or inquiries you did not authorize.

➤ **FREEZE YOUR CREDIT FILE.** You have a right to place a 'security freeze' on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security freeze to take control over who gets access to the personal and financial information in your credit report 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. Note that a security freeze generally does not apply to existing account relationships and when a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a security freeze. To place a security freeze on your credit report, contact each of the 3 major consumer reporting agencies -

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

3 MAJOR CREDIT BUREAUS / CONSUMER REPORTING AGENCIES

Equifax
P.O. Box 105788 Atlanta,
GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.comm

TransUnion
P.O. Box 2000
Chester, PA 19022
1-800-680-7289
www.transunion.com

To request a freeze, you will need to provide the following:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.), Social Security Number, and Date of birth; and
- If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
- Proof of current address such as a current utility bill or telephone bill;
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

If you request a security freeze via toll-free telephone or other secure electronic means, the credit reporting agencies have 1 business day after receiving the request to place the freeze. In the case of a request made by mail, the bureaus have 3 business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within 5 business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receiving a request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have 3 business days after receiving the request to remove the freeze.

➤ **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, 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, which is an alert lasting 7 years. Contact the credit reporting agencies listed above to activate an alert.

➤ **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM FTC.** Go to <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html>. Federal Trade Commission also provides information at www.ftc.gov/idtheft FTC hotline is 877-438-4338; TTY: 1-866-653-4261 or write to FTC, 600 Pennsylvania Ave., NW, Washington, D.C. 20580.

➤ **CONSIDER GETTING AN IDENTITY PROTECTION PIN:** The IRS offers Identity Protection PINs to prevent someone else from filing a tax return using your Social Security number. More information about this offering from the IRS may be found at <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

➤ **FAIR CREDIT REPORTING ACT:** You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list includes the following FCRA rights: (1) To receive a copy of your credit report, which must contain all the information in your file at the time of your request; (2) To receive a free copy of your credit report, at your request, once every 12 months from each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion; (3) To receive a free credit report if a company takes adverse action against you (e.g. denying your application for credit, insurance, or employment), and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft; (4) To ask for a credit score; (5) To dispute incomplete or inaccurate information; (6) To obtain corrections to your report or delete inaccurate, incomplete, or unverifiable information; (7) Consumer reporting agencies may not report outdated negative information; (8) To restrict access to your file and to require consent from you for reports to be provided to employer; (9) To limit "prescreened" offers of credit and insurance you receive based on information in your credit report; and (10) To seek damages from violators. Note - Identity theft victims and active-duty military personnel have additional rights.

- **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM YOUR STATE ATTORNEY GENERAL.**
- *Connecticut: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag*
 - *District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 400 6th Street, NW, Washington, DC 20001, 1-202-727-3400, databreach@dc.gov, www.oag.dc.gov*
 - *Maryland: You may contact and obtain information from your state attorney general at: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-410-528-8662; www.oag.state.md.us Consumer Hotline 1-410-528-8662, or consumer@oag.state.md.us.*
 - *Massachusetts: Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html*
 - *New York: You may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-6971220, <http://www.dos.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>*
 - *North Carolina: You may contact and obtain information from your state attorney general at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699, 1-919-716-6000/ 1-877-566-7226, www.ncdoj.gov*
 - *Rhode Island: Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov. (Approximately 14 Rhode Island residents were impacted by this incident.)*