July 28, 2023

Name
Address
City State Zip

Dear

You are receiving this letter because you have a checking account with Stone Bank. As an abundance of caution, we are writing to tell you about a data security incident that may have allowed an unauthorized individual to acquire your name, checking account number, and other information printed on your checks. We take the protection and proper use of your information very seriously. For this reason, you are being contacted directly to explain the circumstances of the incident.

Our bank uses outside service providers for a variety of banking related services. One service is to clear checks written on or deposited to accounts at this bank. This process is by scanned images of the checks submitted for processing. In this process, scanned images of checks are transferred between financial institutions. The service provider used MOVEit Transfer, a software tool for sending and receiving large data files over the Internet. Progress Software developed MOVEit Transfer. In June 2023, the service provider learned from Progress Software of a vulnerability that *could* allow unauthorized access to servers used to host MOVEit Transfer.

The service provider responded by applying 3 software patches provided by Progress Software and opening an investigation. Law enforcement was notified and data forensic experts were hired to assist in its investigation. The investigation determined that unauthorized individuals had likely used the vulnerability to access the service provider's MOVEit server on May 27, 2023. This *could* have allowed the unauthorized individual to access files stored on the server, which may have included images of your checks and/or your checking account number. However, it has not been determined which files the unauthorized individual acquired.

What information was involved?

Files stored on the MOVEit server included images of checks and checking account number information. In other words, potentially compromised information includes anything printed on the face or the back of the checks, including as applicable the account holder's name, address, routing number, account number and signature. Due to the inability to confirm which files the unauthorized individual acquired, it is unknown whether your account number and other information were among the files acquired by the unauthorized individuals.

What you can do.

You should remain vigilant over the next 12 to 24 months for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. Promptly report incidents of suspected identity theft or suspicious activity to your bank. Also, review the below "Additional Resources" section included in this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. You should also ask your bank about preauthorized checks, ACH debit blocks, and other fraud prevention services.

What is being done.

Law enforcement and federal regulators have been notified regarding this incident. Three software patches provided by Progress Software have been made in an effort to prevent future vulnerabilities, and the service provider is reviewing and updating its security policies and incident response plans to reduce the risk of similar events occurring in the future.

E

For more information.

If you have questions, please call (833) 253-2265, Monday through Friday from 8:00 a.m. to 5:00 p.m. CST. You may also reach us at customerservice@stonebank.com.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:
Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a free copy of your credit report once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze: (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. Each copy must be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).