

July 31, 2024

VIA EMAIL

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

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP, represents the State Bank of Taunton (“SBT”) in connection with a recent data security incident described in greater detail below. This notice is being sent because personal information for Maryland residents may have been involved in the incident. The purpose of this letter is to notify you of the incident in accordance with Maryland’s data breach notification statute Md. Code Ann. Comm. Law §§ 14-3501 - 3508.

1. Nature of the Security Incident

On January 11, 2024, SBT became aware of unusual network activity and immediately took steps to secure its systems. SBT engaged cybersecurity experts to assist with the process. The investigation determined that certain SBT data may have been acquired without authorization on or around January 11, 2024. After undertaking a review of the potentially affected files, SBT identified certain personal information that may have been involved. SBT’s review concluded on July 25, 2024 and revealed the individuals whose personal information could have been involved.

2. Number of Maryland Residents Involved

Beginning July 31, 2024, SBT notified 1 Maryland 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.

The personal information involved in this incident includes individuals’ names and social security numbers.

3. Steps Taken to Address the Incident

As soon as the SBT discovered this unusual network activity, it took steps to secure the affected systems and launched an investigation to determine whether, and to what extent, personal information had been accessed or acquired without authorization. SBT has also implemented additional security measures in an effort to prevent a similar incident from occurring in the future. Further, as referenced in the sample consumer notification letter, the SBT has offered individuals 12 months of complimentary services through IDX, which include Credit Monitoring, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

SBT has established a toll-free call center through IDX to answer questions about the incident and address related concerns.

4. Contact Information

SBT 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 jcherry@constangy.com.

Sincerely,



Jason Cherry
Partner
Constangy, Brooks, Smith & Prophete, LLP

Enclosure: Sample Notification Letter



P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

July 31, 2024

Subject: Notice of Data <<Variable Text 1: Breach or Security Incident>>

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

We are writing to inform you about a recent data security incident experienced by the State Bank of Taunton (“SBT”), that may have affected your personal information. SBT takes the privacy and security of all 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 information.

What Happened. On January 31, 2024, SBT discovered unauthorized activity within its digital environment. In response, SBT took steps to secure its network and began an investigation. SBT also engaged independent cybersecurity experts to assist with the investigative efforts. This investigation determined that unauthorized access to certain portions of our network occurred on January 31, 2024. Following a thorough and time-intensive review of the affected data, SBT learned on <<Address_LOOKUP_DATE>> that your personal information was potentially affected by this incident. Please note that SBT has no evidence of the misuse or attempted misuse of any potentially impacted information.

What Information Was Involved? The information potentially impacted in connection with this incident included your name and <<Breached Elements>>.

What Are We Doing? As soon as SBT discovered this incident, it took the steps described above. In addition, SBT has implemented measures to enhance the security of its digital environment in an effort to minimize the risk of a similar incident occurring in the future.

In addition, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. The deadline to enroll in IDX services is October 31, 2024.

What You Can Do: You can follow the recommendations on the following page to help protect your personal information. SBT also encourages you to enroll in the complimentary services offered to you through IDX by using the enrollment code noted above.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, IDX representatives have been fully briefed on the incident and are prepared to assist you with any questions. Please call 1-800-939-4170 from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays).

Please accept my sincere apologies and know that SBT takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

Duane Peterson

President
State Bank of Taunton
101 N. Main St.
P.O. Box 398
Taunton, MN 56291

STEPS YOU CAN TAKE TO HELP 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:

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 your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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: 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 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
www.ftc.gov/idtheft
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

Rhode Island: The total number of individuals receiving notification of this incident is <<#>>.

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 <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.