



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Richard Aponte-Boyd
Office: (267) 930-4888
Fax: (267) 930-4771
Email: raponte@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

August 12, 2022

VIA E-MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent Lone Star Capital Bank, N.A. ("Lone Star") located at 150 N Loop 1604 E, San Antonio, TX 78232, and write to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maryland resident. By providing this notice, Lone Star does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about May 31, 2022, Lone Star identified suspicious activity related to an employee's email account. Upon learning of the suspicious activity, Lone Star immediately took steps to secure the email account and launched an investigation, with the assistance of third-party computer experts, to determine the nature and scope of the event. Through the investigation, Lone Star determined that the employee's email account was subject to unauthorized access on May 31, 2022. As such, Lone Star reviewed the contents of those files to determine what information was contained therein and to whom it related for purposes of providing notification.

The information that could have been subject to unauthorized access includes name, and Social Security number.

Notice to Maryland Resident

On or about August 12, 2022, Lone Star provided written notice of this incident to one (1) Maryland resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Lone Star moved quickly to investigate and respond to the incident, assess the security of Lone Star systems, and identify the potentially affected individual. Further, Lone Star notified federal law enforcement regarding the event. Lone Star is also working to implement additional safeguards and training to its employees. Lone Star is providing access to credit monitoring services for twelve (12) months, through Experian, to the individual whose personal information was potentially affected by this incident, at no cost to this individual.

Additionally, Lone Star is providing the impacted individual with guidance on how to better protect against identity theft and fraud, including advising the individual to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Lone Star is providing the individual with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Lone Star is providing written notice of this incident to other relevant state and federal regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4888.

Very truly yours,

Richard Aponte-Boyd of
MULLEN COUGHLIN LLC

RAB/aml
Enclosure

EXHIBIT A



Return Mail Processing
PO Box 999
Suwanee, GA 30024

August 12, 2022

2 1 482 *****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



NOTICE OF [EXTRA1]

Dear Sample A. Sample:

Lone Star Capital Bank N.A. ("LSCB") is writing to inform you of a recent event that may have impacted some of your information. Although there is no indication that your information has been misused in relation to this event, we are providing you with information about the event, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened. On or about May 31, 2022, LSCB became aware of suspicious activity relating to an employee email account. LSCB immediately took steps to secure email accounts and launched an investigation, which included working with third-party experts, to determine the nature and scope of the activity. LSCB's investigation determined that there was unauthorized access to certain email accounts on May 31, 2022. However, the forensic investigation was unable to determine whether there was access to specific emails and attachments within the account.

In an abundance of caution, LSCB reviewed the contents of the email account to determine what information was impacted and to whom the information relates. We are notifying you because that investigation determined certain information related to you may have been impacted.

What Information Was Involved. The information that may have been impacted by this incident includes your [Extra2], and name. At this time, we have no indication that your information was subject to actual or attempted misuse as a result of this incident.

What We Are Doing. Data privacy and security are among LSCB's highest priorities, and there are measures in place to protect information in LSCB's care. Upon discovery, LSCB promptly commenced an investigation with the assistance of third-party cyber security specialists to confirm the nature and scope of this incident. This investigation and response included confirming the security of our systems, reviewing the contents of relevant data for sensitive information, and notifying impacted individuals associated with that sensitive information. As part of our ongoing commitment to the privacy of information in our care, we are reviewing our policies procedures and processes related to the storage and access of information, and additional workforce training is being conducted to reduce the likelihood of a similar future event. We also notified regulatory authorities, as required by law.

As an added precaution, we are also offering twelve (12) months of complimentary access to credit monitoring services through Experian. Individuals who wish to receive these services must enroll by following the attached enrollment instructions.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, explanation of benefits, and credit reports for suspicious activity over the next 12 to 24 months. You may also review the information contained in the attached *Steps You Can Take to Help Protect Your Information* to learn helpful tips on steps you can take to protect against possible misuse should you feel it appropriate to do so. There you will find more information on the credit monitoring services we are making available to you. While LSCB will cover the cost of these services, you will need to complete the activation process.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please call our dedicated assistance line at (855) 726-7329, toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide engagement number B058786. You can also write to us at 150 N Loop 1604 E, San Antonio, TX 78232.

Sincerely,

Lone Star Capital Bank, N.A.

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for twelve (12) months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for twelve (12) months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary twelve (12) month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by November 30, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(855) 726-7329** by **November 30, 2022**. Be prepared to provide engagement number **B058786** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR TWELVE (12) MONTHS EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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

** 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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a 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 a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer’s 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 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. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); 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 credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 and your state Attorney General. This notice has not been delayed by law enforcement.

For California residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For Maryland residents: the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

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 All U.S. residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338).