December 29, 2023

VIA ELECTRONIC MAIL

Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP represents Lavaca County, Texas (the "County") in connection with a data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with New Hampshire's data breach notification statute.

1. Nature of the Security Incident

On October 20, 2023, the County became aware of suspicious activity in its email environment. In response, the County immediately took steps to secure its digital environment, including performing a password reset and engaging a leading cybersecurity firm to assist with an investigation. Through the investigation, the County learned that one (1) employee email account may have been subject to access by an unauthorized individual. The County subsequently conducted a comprehensive review of the affected data on the email account, and, on November 21, 2023, the County determined that personal information belonging to certain individuals may have been affected. Additionally, the County began the process of locating relevant mailing information to effectuate notification to such individuals, which was completed on December 20, 2023.

The information affected may have included . Please note that the County has no current evidence to suggest misuse or attempted misuse of personal information involved in the incident.

2. Number of New Hampshire Residents Involved

On December 29, 2023, the County notified one (1) New Hampshire resident of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the impacted individual is included with this correspondence.

3. Steps Taken to Address the Incident

In response to the incident, the County is providing individuals with information about steps that they can take to help protect their personal information, and, out of an abundance of caution, it is also offering individuals complimentary credit monitoring and identity protection services through IDX, a ZeroFox company. The call center is available Monday through Friday from 8:00am to 8:00pm Central Time. Additionally, to help reduce the risk of a similar future incident, the County has implemented additional technical security measures throughout its email environment.

4. Contact Information

The County 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 .

Sincerely,

Lindsay B. Nickle
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Enclosure: Sample Notification Letter

4145 SW Watson Ave
Suite 400
Beaverton, OR 97005

Family or Representative of
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

December 29, 2023

Subject: Notice of Data <<Variable Text 1 – Subject Line>>

Dear Family or Representative of <<First Name>> <<Last Name>>:

We are writing to inform you of a recent data security incident experienced by Lavaca County, Texas ("Lavaca County") that may have involved your family member's personal information. Lavaca County takes the privacy and security of all information in our possession very seriously. This is why we are notifying you about the incident, providing you with steps you can take to help protect your family member's personal information, and offering you the opportunity to enroll in complimentary identity protection services.

What Happened. On October 20, 2023, Lavaca County experienced suspicious activity within our email environment and immediately initiated an investigation of the matter, including engaging cybersecurity experts to assist with the process. On or around October 25, 2023, the investigation confirmed that one (1) County employee's email account may have been accessed without authorization. After a comprehensive review of all information contained in that employee's mailbox, on November 21, 2023, some of your family member's personal information was identified as being contained within the potentially affected data. We then worked to obtain all missing address information to effectuate notification to such individuals, which was completed on December 20, 2023.

What Information Was Involved. The information may have included your family member's <<Variable Text 2 – Impacted Data>>. Please no that we have no evidence to suggest any misuse or attempted misuse of information potentially involved in the incident.

What We Are Doing. As soon as we discovered the incident, we took the steps described above and implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future. We are also offering your family member complimentary identity protection services through IDX, which are free upon enrollment. These services include <<12 months / 24 months>> of CyberScan dark web monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your family member's identity is compromised.

What You Can Do. We recommend you read the guidance included with this letter about additional steps you can take to protect your family member's information. In addition, we encourage you to enroll in the identity theft protection services we are offering through IDX at no cost to you.

You can enroll in the IDX identity protection services by calling 1-800-939-4170 or by going to https://app.idx.us/account-creation/protect or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. Please note the deadline to enroll is March 29, 2024.

For More Information. If you have questions, please call IDX at 1-800-939-4170, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. IDX representatives are fully versed on this incident and can answer questions you may have regarding the protection of your family member's personal information.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

Keith Mudd
County Judge

Lavaca County, Texas
109 N. La Grange Street
Hallettsville, TX 77964

Steps You Can Take To Protect Your Family Member's 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 family member's account statements and credit reports closely. If you detect any suspicious activity on an account related to your family member, 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: In order to obtain a copy of your family member's credit report, you will need to provide proof that you are authorized to act on their behalf. This often occurs when the credit bureau is initially informed of their passing with a copy of their death certificate, and a copy of the legal document authorizing you to act on their behalf. You may then obtain a free copy of your family member's credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 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 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You should inform the credit reporting agencies that your family member is deceased, and you can do so with a copy of their death certificate and a copy of the legal document authorizing you to act on their behalf. You may then inform the credit reporting agencies of fraudulent activity that may involve your family member's identify. You may also want to consider placing a fraud alert on your own 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 family member's credit file for up to one year at no cost. This will prevent new credit from being opened in your family member's 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 family member's credit report without your consent. You must separately place a security freeze on your family member's 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 your family member including their full name, Social Security Number, date of birth, current and previous addresses, and copy of their state-issued identification card.

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

Texas Attorney General
PO Box 12548
Austin, TX 78711
texasattorneygeneral.gov
1-800-621-0508

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
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

Consumers have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in their file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and consumer rights pursuant to the FCRA, please visit https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.