Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

File No. 3842.67

November 23, 2022

VIA ELECTRONIC MAIL
Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 0330
Email: DOJ-CPB@doj.nh.gov

Re: **Notice of Data Security Incident**

Dear Attorney General Formella:

Lewis Brisbois Bisgaard & Smith LLP ("Lewis Brisbois") represents Johnson County, Texas (the "County"), in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with the New Hampshire data breach notification statute.

1. Nature of the Security Incident

On July 7, 2022, the County became aware of a file belonging to the County that may have been obtained by an unauthorized actor. In response, the County immediately took steps to secure its digital environment and engaged a leading cybersecurity firm to assist with an investigation. This investigation determined that one file belonging to the County was inadvertently left publicly available during a data migration project and may have been accessed without authorization as a result. The County completed a comprehensive review of the potentially affected data and determined personal information for certain individuals may have been involved in this incident. The County engaged a vendor to gather up-to-date contact information in order to provide notification to potentially affected individuals and concluded this process on October 17, 2022.

Please note this incident was limited to a file obtained from a third-party website. The investigation did not identify any evidence of impact to the County's own environment. Additionally, the County is not aware of any misuse or attempted misuse of information. These individuals were notified through U.S. First-Class Mail on November 23, 2022. Additionally, the County posted notice of the data security incident on the home page of its website.

The impacted information includes full name, address, Social Security number, and date of birth. To date, the County has no evidence that any potentially impacted information has been misused in conjunction with this incident.

2. Number of New Hampshire Residents Affected

The County notified thirty-three (33) New Hampshire residents of this data security incident via U.S. First-Class Mail on November 23, 2022. A sample copy of the notification letter sent to the affected individuals is included in this letter.

3. Steps Taken Relating to the Incident

The County has implemented additional security measures to secure its digital environment and reduce the risk of a similar incident occurring in the future and to protect the privacy and security of all personal information in its possession. In addition, the County has offered complimentary credit and identity monitoring services through IDX to the notified individuals. The County has also established a toll-free call center through IDX to answer any questions about the incident and address related concerns. The call center is available Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time.

4. Contact Information

The County remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at 214.722.7141 or via email at Lindsay.Nickle@lewisbrisbois.com.

Very truly yours,

Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

LBN/rlw
Encl: Sample Consumer Notification Letter

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

To Enroll, Please Call:
(833) 814-1734
Or Visit:
https://response.idx.us/JohnsonCounty
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

November 23, 2022

Re: Notice of Data <<Variable Text 1>>

Dear <<FIRST NAME>> <<LAST NAME>>,

We are writing to provide you with information about a recent data security incident that may have involved your personal information. Johnson County (the "County") strives to maintain the privacy and security of all information within our possession. We are writing to notify you of this incident, offer you complimentary identity monitoring services, and inform you about steps you can take to help safeguard your personal information.

What Happened. On July 7, 2022, the County became aware of a file belonging to the County that may have been obtained by an unauthorized actor. In response, we immediately took steps to secure our digital environment and engaged a leading cybersecurity firm to assist with an investigation. This investigation determined that one file belonging to the County was inadvertently left publicly available during a data migration project and may have been accessed without authorization as a result. We completed a comprehensive review of the potentially affected data and determined some of your personal information may have been involved in this incident. We engaged a vendor to gather up-to-date contact information in order to provide notification to potentially affected individuals. We concluded this process on October 17, 2022. Please note this incident was limited to a file obtained from a third-party website. The investigation did not identify any evidence of impact to the County's own environment. Additionally, the County is not aware of any misuse or attempted misuse of information.

What Information Was Involved. The potentially affected information may have included your name, address, Social Security number, and date of birth.

What We Are Doing. As soon as we discovered this incident, we took the steps described above. As part of the response process, we implemented additional measures to reduce the risk of a similar incident occurring in the future.

Additionally, the County is providing you with information about steps that you can take to help protect your personal information and, as an added precaution, is offering you complimentary identity theft protection services through IDX. These identity protection services include: <<12/24>> months of credit and CyberScan 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 identity is compromised.

What You Can Do. We recommend that you activate your complimentary IDX services by calling (833) 814-1734 or going to https://response.idx.us/JohnsonCounty and using the enrollment code provided above. Representatives are available from 8:00 a.m. to 8:00 p.m. Central Time from Monday to Friday. Please note that deadline to enroll is February 23, 2023. In addition, we recommend that you review the guidance included with this letter about additional steps you can take to protect your personal information.

For More Information. If you have questions or need assistance, please contact IDX at (833) 814-1734, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time, excluding major U.S. holidays. IDX representatives are fully versed on this incident and can answer questions you may have regarding the protection of your personal information.

Johnson County takes this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerelv

Roger Harmon
County Judge

Johnson County
2 North Main Street
Cleburne, Texas 76033

Steps You Can Take to Protect Your Personal 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 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-800-831-5614
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 csredit 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
1-877-438-4338

Maryland Attorney General
St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

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
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

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://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.