



Lindsay B. Nickle, Partner, Vice Chair
Cybersecurity & Data Privacy Team
100 Crescent Court, Suite 700
Dallas, Texas 75201
LNickle@constangy.com
Direct: 806.535.0274

March 4, 2025

VIA ONLINE PORTAL

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs Response Team
2115 State Capital
Lincoln, NE 68509

Re: Notice of Data Security Incident

To Attorney General Hilgers:

Constangy, Brooks, Smith & Prophete, LLP represents Duval County, Texas ("Duval 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 Nebraska's data breach notification statute.

Nature of the Security Incident

On August 23, 2024, Duval County experienced suspicious activity within its email environment. In response, Duval County immediately took steps to secure its email tenant and engaged a leading cybersecurity firm to assist with an investigation and determine whether sensitive or personal information may have been accessed or acquired during the incident. Through the investigation, Duval County identified that certain information within one (1) employee's mailbox account may have been acquired without authorization. Duval County then engaged an independent team to conduct a comprehensive review of all data within the affected mailbox, and on October 21, 2024, that review determined that the personal information of a limited number of individuals associated with Duval County may have been affected. Duval County then worked diligently to obtain missing address information for those affected individuals to effectuate notification, which was completed on February 21, 2025.

The information affected may have included name, date of birth, and driver's license and/or state identification number.

Number of Nebraska Residents Involved

On March 4, 2025, Duval County notified one (1) Nebraska resident 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.

Steps Taken to Address the Incident

In response to the incident, Duval 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 identity protection services. These include 12 months of credit monitoring and CyberScan dark web monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. Duval County is also providing a dedicated call center to address any questions individuals may have relating to the incident, which will remain operational for ninety (90) days. Additionally, to help reduce the risk of a similar future incident, Duval County has implemented additional technical security measures throughout the environment.

Contact Information

Duval 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 LNickle@Constangy.com.

Sincerely,



Lindsay B. Nickle
Constangy, Brooks, Smith & Prophete, LLP

Enclosure: Sample Notification Letter



Secure Processing Center:
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>> or <<IMB>>

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

March 4, 2025

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

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a recent data security incident experienced by Duval County, Texas (“Duval County”) that may have involved your personal information. Duval 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 personal information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened. On August 23, 2024, Duval 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. As a result of the investigation, we identified that the contents of an employee’s email account may have been acquired without authorization. We then conducted a comprehensive review of the information contained in that employee’s mailbox, and on October 21, 2024, certain personal information was identified as within the potentially affected data. We then worked to obtain all missing address information so that we could complete notification to affected individuals. This process was completed on February 21, 2025.

What Information Was Involved. The information may have included your name, [Variable Text 2 – Impacted Data]. Please note 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 you complimentary credit monitoring and identity protection services through IDX. These services are free to you upon enrollment and include <<12 months / 24 months>> of credit and 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 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 information. In addition, we encourage you to enroll in the credit monitoring and identity theft protection services we are offering through IDX at no cost to you. To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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> 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 June 4, 2025.

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 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,

Arnoldo Cantu
County Judge

Duval County, Texas
400 E. Gravis St
San Diego, TX 78384

STEPS YOU CAN TAKE TO HELP 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 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
1-833-799-5355
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

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

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/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.