



Denton County Commissioners Court  
 110 West Hickory Street  
 Denton, TX 76201-4168

August 27, 2021

G7209-L01-0000001 T00001 P001 \*\*\*\*\*SCH 5-DIGIT 32808



SAMPLE A. SAMPLE - L01  
 APT ABC  
 123 ANY ST  
 ANYTOWN, ST 12345-6789

**ENGAGEMENT NUMBER: B016808**



**RE: NOTICE OF Extra1**

Dear Sample A. Sample:

Denton County, Texas (“The County”) is writing to inform you of a recent incident that may have impacted the security of your personal health information. We take this incident very seriously and are providing you with information about the incident, our response, and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

**What Happened?** On July 7, 2021, The County became aware of a vulnerability within the third-party provider application utilized by The County for its COVID-19 vaccination clinics that potentially exposed individual’s data hosted on the system to anonymous users. We **immediately** shut down the third-party application and launched an investigation to assess the nature and scope of the vulnerability. The investigation confirmed that there was a configuration error on the third-party application that potentially exposed individual’s health information to anonymous public users. While the County has no evidence of actual or attempted misuse of any information, we could not rule out the possibility of access to data present in the database. The County undertook a lengthy and labor-intensive process to identify the health information impacted in the database. The only health information potentially impacted was COVID-19 vaccination data. **The County never collected social security numbers, driver license numbers, or financial account information.**

**What Information Was Involved?** Our investigation revealed that the database contained your name, date of birth, phone number, COVID-19 vaccination data, and email address. Although this information may have been accessible, there is no indication that this information was misused. However, we are notifying you of this incident in an abundance of caution.

**What We Are Doing.** The confidentiality, privacy, and security of health information within our care is among The County’s highest priorities. Upon learning of this incident, we immediately disabled the third-party application utilized by The County for its COVID-19 vaccination clinics and commenced an investigation to ensure the security of the third-party application prior to reinstating The County’s use of the application. Since the incident, we have also worked internally and with the third-party provider to implement additional security measures to increase the security of the third-party provider application utilized by The County.

**What You Can Do.** While The County is not aware of any actual or attempted misuse of information as a result of this incident, we nonetheless encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and to monitor your credit reports for suspicious activity. Please review the enclosed “Steps You Can Take to Protect Personal Information”, which contains information on what you can do to better protect against possible misuse of your information.

0000001



**For More Information.** We understand you may have questions about this incident that are not addressed in this letter. We've set up a dedicated assistance line to answer your privacy questions. If you have additional questions or concerns, please call us toll-free at (877) 659-0604, 8:00 AM to 10:00 PM Central Time, Monday through Friday, and 10:00 AM to 7:00 PM Central Time, Saturday through Sunday (excluding U.S. holidays).

Denton County, Texas

## STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

### 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](http://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:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
888-298-0045	1-888-397-3742	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](http://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 District of Columbia residents*, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and [oag@dc.gov](mailto:oag@dc.gov).

*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](http://www.oag.state.md.us). The County is located at 110 West Hickory Street, Denton, TX 76201-4168.

*For New Mexico residents*, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

*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 North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and [www.ncdoj.gov](http://www.ncdoj.gov).

*For Rhode Island residents*, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; [www.riag.ri.gov](http://www.riag.ri.gov); and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 5 Rhode Island residents impacted by this incident.

**DENTON COUNTY, TEXAS – NOTICE OF DATA EVENT**  
**August 24, 2021**

Denton County, Texas (“The County”) is providing notice of a recent incident that may have impacted the security of personal health information. The County takes this incident very seriously and this notification provides information about the event, The County’s response to it, and resources available to individuals to help protect their information, should they feel it necessary to do so.

**What Happened?** On July 7, 2021, The County became aware of a vulnerability within the third-party provider application utilized by The County for its COVID-19 vaccination clinics that potentially exposed individual’s data hosted on the system to anonymous users. The County immediately shut down the third-party application and launched an investigation to assess the nature and scope of the vulnerability. The investigation confirmed that there was a configuration error on the third-party application that potentially exposed individual’s health information to anonymous public users. While The County has no evidence of actual or attempted misuse of any information, The County could not rule out the possibility of access to data present in the database. The County undertook a lengthy and labor-intensive process to identify the health information impacted in the database. The only health information potentially impacted was COVID-19 vaccination data. The County never collected social security numbers, driver license numbers, or financial account information.

**What Information Was Involved?** The information that may have been subject to unauthorized access for each potentially affected individual includes name, date of birth, email, phone number, and COVID-19 vaccination information. Although this information may have been accessible, there is no indication that this information was misused. However, in an abundance of caution, The County is in the process of notifying individuals whose information was involved.

**What Is The County Doing?** Upon learning of this incident, The County immediately disabled the third-party application utilized by The County for its COVID-19 vaccination clinics and commenced an investigation to ensure the security of the third-party application prior to reinstating The County’s use of the application. Since the incident, The County has also worked internally and with the third-party provider to implement additional security measures to increase the security of the third-party provider application utilized by The County.

**What You Can Do?** While The County is not aware of any actual or attempted misuse of information as a result of this incident, The County nonetheless encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and to monitor your credit reports for suspicious activity. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
888-298-0045	1-888-397-3742	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

## DENTON COUNTY TEXAS LOGO

Individuals can further educate themselves regarding identity theft, fraud alerts, security freezes, and steps to protect their information by contacting the Federal Trade Commission or the Texas Attorney General. Instances of known or suspected identity theft should be reported to law enforcement and the state attorney general.

The County regrets any concern this incident may cause. If individuals have questions about this incident, they may contact The County's toll-free dedicated assistance line at 877-659-0604. When contacting the toll-free number please reference engagement number B017844. This toll-free line is available 8:00 AM to 10:00 PM Central Time, Monday through Friday, and 10:00 AM to 7:00 PM Central Time, Saturday through Sunday (excluding U.S. holidays). Individuals may also write to The County at 110 West Hickory Street, Denton, TX 76201-4168.