

July 10, 2024

Via E-MAIL

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

Re: Notice of Security Incident

To Whom It May Concern:

We are providing the following notice of a security incident on behalf of our client, Dallas County, Texas. Although the impacted information varies based on the individual at issue and their relationship with the County, this incident impacted 37 Maryland residents.

The County began notifying impacted individuals of the incident on July 10, 2024, through various communication channels, including through a nationwide media press release, website notice, and postal mail.

What Happened?

As the County previously shared with its residents and partners, on October 19, 2023, the County became aware of a cybersecurity incident affecting a portion of its environment. Upon detection, the County promptly took steps to contain the incident and engaged third-party cybersecurity specialists to perform a comprehensive investigation, including to determine what data may be involved.

Dallas County initially provided notice of this incident on October 31, 2023, through its dedicated website. On January 9, 2024, Dallas County updated its website to provide individuals with information on how to protect their personal information and an offer for complimentary credit monitoring for any individual concerned about the incident or their information while the County completed its investigation.

The County recently completed its investigation and is now actively notifying impacted individuals through various communication channels. This includes notice through nationwide media, an update to its dedicated website (www.dallascounty.org/about-us/hot-links/notice-cybersecurity-incident.php), and letter mail for individuals whose contact information was available. The County is also offering two years of complimentary credit monitoring and identity theft protection services to individuals whose Social Security or taxpayer identification numbers were involved.

What Information Was Involved?

The County might hold information about individuals for several reasons: they could be a resident, an employee, or they might have received services from or interacted with one of the County's agencies (e.g., Department of Health and Human Services). Additionally, the County participates in data sharing agreements with other organizations to enhance the services offered to its residents and the public.

Although the information affected by this incident varies based on the individual and their association with the County, this incident primarily involved the following information: name; Social Security number (SSN); date of birth; driver's license/state identification number; and taxpayer identification number. For some individuals, certain types of medical information (e.g., diagnosis or conditions information) and health insurance information may be involved.

Remedial Steps Taken

Upon becoming aware of the incident, the County promptly initiated measures to secure its information. This included an extensive deployment of an Endpoint Detection and Response (EDR) tool across servers and endpoints connected to County networks, forcing password changes for all users to grant access to its systems, and blocking ingress and egress traffic to IP addresses identified as malicious, among others. The County also engaged external cybersecurity specialists to investigate the nature and scope of the incident and conduct a comprehensive investigation to determine what information was involved.

The County established a dedicated call center for individuals to call with any questions or concerns relating to the incident. The phone number is 1-888-330-2852 and representatives are available Monday through Friday, 9 AM to 9 PM ET. Individuals may also visit Dallas County's dedicated website, available at <https://www.dallascounty.org/about-us/hot-links/notice-cybersecurity-incident.php>, for the latest information pertaining to this incident.

Should you have any questions or concerns about this matter, please do not hesitate to contact me using the information provided below.

Sincerely,

A handwritten signature in black ink, appearing to read "Sadia Mirza".

Sadia Mirza
Direct: 949.622.2786
Email: sadia.mirza@troutman.com



PO Box 480149
Niles, IL 60714

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>
<<Country>>

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

July 10, 2024

Notice of Data Breach

Dear <<Name 1>> <<Name 2>>,

Dallas County, Texas ("the County") writes to inform you about a recent security incident that may impact the confidentiality of information related to you. We encourage you to read this letter carefully as it contains important information regarding the incident, our response, and steps you can take to help protect your personal information.

What Happened?

As the County previously shared with its residents and partners, on October 19, 2023, the County became aware of a cybersecurity incident affecting a portion of its environment. Upon detection, the County promptly took steps to contain the incident and engaged third-party cybersecurity specialists to perform a comprehensive investigation, including to determine what data may be involved.

During the investigation, the County established a dedicated call center for individuals to call should they have any questions relating to the incident. The call center continues to be operational as of the date of this letter.

The County recently completed its investigation and determined that your information may be involved. The specific information impacted as it relates to you is detailed further below.

What Information Was Involved?

The County might hold information about you for several reasons: you could be a resident, an employee, or you might have received services from or interacted with one of our agencies (e.g., Department of Health and Human Services). Additionally, the County participates in data sharing agreements with other organizations to enhance the services we offer to our residents and the public.

The specific information affected by this incident depends on the individual and their association with the County. After reviewing our records, we have determined that your information, which may have been involved, includes your name and <<Variable Data>>.

What Are We Doing?

Upon becoming aware of the incident, the County promptly initiated measures to secure its information. This included an extensive deployment of an Endpoint Detection and Response (EDR) tool across servers and endpoints connected to our

network, forcing password changes for all users to grant access to our systems, and blocking ingress and egress traffic to IP addresses identified as malicious, among others. The County also engaged external cybersecurity experts to investigate the nature and scope of the incident and conduct a comprehensive investigation to determine what information was involved.

The County has arranged for IDX, a third-party vendor, to provide individuals whose Social Security Number or Tax Identification Number may have been impacted by this incident with 24 months of complimentary identity protection services. A description of the benefits and enrollment instructions is provided below.

What Can You Do?

The County encourages you to consider the following recommendations to protect your personal information:

1. **Register for Identity Protection Services.** We have arranged for IDX to provide individuals whose Social Security Number or Tax Identification Number may have been impacted by this incident with 24 months of complimentary identity protection services. Please note the deadline to enroll is October 10, 2024. These services provide access to the following:
 - **Single Bureau Credit Monitoring (for adults).** Monitoring of credit bureau for changes to your credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in your credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities.
 - **CyberScan.** Dark web monitoring of underground websites, chat rooms, and malware to identify trading or selling of personal information.
 - **Identity Theft Insurance.** Identity theft insurance will reimburse you for expenses associated with restoring your identity should you become a victim of identity theft. If your identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best “A-rated” carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.
 - **Managed Identity Recovery Service.** This service provides restoration for identity theft issues such as: account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation.

Enrollment Instructions: Using your unique enrollment code, <<enrollment code>>, you may enroll in the service three ways:

- **Online:** Visit <https://app.idx.us/account-creation/protect> and follow the instructions to enroll. Please note that you will be asked to create an account and complete an identity verification process to enroll in the service.
 - **By Phone:** We encourage you to contact IDX with any questions, including with respect to the complimentary identity protection services, by calling 1-888-330-2852. IDX representatives are available Monday through Friday from 9 AM to 9 PM Eastern Time. Remember to have your code handy when you're ready to enroll.
 - **By QR Code:** You may scan the QR code found at the top of this letter which will direct you to the enrollment website to enroll.
2. **Review Your Accounts for Suspicious Activity.** We encourage you to remain vigilant by regularly reviewing your accounts and monitoring credit reports for suspicious activity.
 3. **Order A Credit Report.** If you are a U.S. resident, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. Contact information for the nationwide credit reporting agencies is provided in the next section.

4. **Contact the Federal Trade Commission, Law Enforcement, and Credit Bureaus.** You may contact the Federal Trade Commission (“FTC”), your state’s Attorney General’s office, or law enforcement, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC’s websites at www.identitytheft.gov and www.ftc.gov/idtheft; call the FTC at (877) IDTHEFT (438-4338); or write to: FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may contact the nationwide reporting agencies at:

- a) Equifax: (800) 525-6285; P.O. Box 740241, Atlanta, Georgia, 30374; or www.equifax.com.
 - b) Experian: (888) 397-3742; P.O. Box 9701, Allen, TX 75013; or www.experian.com.
 - c) TransUnion: (800) 916-8800; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022; or www.transunion.com.
5. **Additional Rights Under the FCRA.** 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 agencies 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 violators. 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: (i) visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf; or (ii) by writing to Consumer Financial Protection Bureau, 1700 G Street, N.W., Washington, DC 20552.

6. **Request Fraud Alerts and Security Freezes.** You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105788
Atlanta, GA 30348
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion LLC

P.O. Box 6790
Fullerton, PA 92834-6790
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
<http://www.transunion.com/creditfreeze>
1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

7. **For Iowa Residents.** You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.
8. **For Maryland Residents.** You can obtain information about avoiding identity theft from the Maryland Attorney General at: Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place Baltimore, MD 21202, (888) 743-0023 (toll-free in Maryland), (410) 576-6300, www.marylandattorneygeneral.gov.
9. **For New York Residents.** You can obtain information about security breach response, identity theft prevention, and identity protection information from the New York State Office of the Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755 (toll-free), 1-800-788-9898 (TDD/TTY toll-free line), <https://ag.ny.gov/>, and at: Bureau of Internet and Technology (BIT), 28 Liberty Street, New York, NY 10005, Phone: (212) 416-8433, <https://ag.ny.gov/internet/resource-center>.
10. **For North Carolina Residents.** You can obtain information about avoiding identity theft from the North Carolina Attorney General at: North Carolina Attorney General's Office 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free in North Carolina), (919) 716-6400, www.ncdoj.gov.
11. **For Residents of Oregon.** You may report suspected identity theft to law enforcement, including the Office of the Oregon Attorney General and the FTC. Contact information for the FTC is included in your notice. The Office of the Oregon Attorney General can be reached: (1) by mail at 1162 Court St. NE, Salem, OR 97301; (2) by phone at (877) 877-9392; or (3) online at <https://www.doj.state.or.us/>.
12. **For Rhode Island Resident.** You can obtain information about avoiding identity theft from the Rhode Island Office of the Attorney General at: Rhode Island Office of the Attorney General, Consumer Protection Unit 150, South Main Street, Providence, RI 02903, (401)-274-4400, www.riag.ri.gov. You have the right to obtain a police report, and to request a security freeze (charges may apply), as described above. Information pertaining to approximately <2> Rhode Island residents was potentially involved in this incident.
13. **For Washington, D.C. Residents.** You can obtain information about avoiding identity theft from the Office of the Attorney General for the District of Columbia at: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202)-727-3400, www.oag.dc.gov. You have the right to request a security freeze (without any charge) as described above.

Other Important Information.

The County established a dedicated call center for individuals to call with any questions or concerns relating to the incident. The phone number is 1-888-330-2852 and representatives are available Monday through Friday, 9 AM to 9 PM ET. You may also write to the County at 500 Elm Street, 7th Floor, Suite 7600, Dallas, TX 75202 with any questions or concerns.

Sincerely,

Dallas County

