April 1, 2025

Notice of Data Security Incident Related to Police Records

We are posting this notice to provide important information regarding a recent cybersecurity incident at doc2e-file, Inc. ("Doc2") involving information pertaining to the City of Lake Jackson, Texas ("Lake Jackson"). We want to provide details about the incident and let our community and others know that we continue to take significant measures to protect the information in our possession.

On September 3, 2024, Lake Jackson received a notification from document management vendor, Doc2, informing Lake Jackson that Doc2 had recently discovered a cyber incident that impacted Doc2's network. Upon receiving this notice, Lake Jackson immediately began an internal investigation and engaged third party cybersecurity experts to determine what information of Lake Jackson's was impacted by this incident. Following an extensive investigation and review, Lake Jackson determined that some of its data was potentially accessed by an unauthorized party as a result of Doc2's incident. The information potentially impacted includes full names along with one or more of the following: Social Security number, date of birth, financial account number, credit card number, and/or debit card number.

While Lake Jackson has no evidence to indicate that any of this information has been or will be misused as a result of this incident, out of an abundance of caution, Lake Jackson wants to make individuals aware of the incident so they can take steps to further protect their information. Lake Jackson will be providing notification to impacted individuals. Lake Jackson also notified and is cooperating with law enforcement in connection to this incident. Please note the type of information impacted varied depending on the individual. Please consult the notice you received or call 855-374-6939 to confirm what information was impacted.

Lake Jackson is committed to protecting the privacy and integrity of the data it maintains. Lake Jackson continues to evaluate and modify practices and internal controls to enhance the security and privacy of personal information in its possession.

The additional information below provides precautionary measures that persons can take to protect their information, including tips for protecting against identity theft and best practices in protecting against financial fraud. While we have no evidence of misuse, it is always important to remain vigilant.

If you have any questions regarding this incident, please call the dedicated and confidential toll-free response line at 855-374-6939. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against potential misuse of your information. The response line is available from 9:00am to 9:00pm ET, Monday through Friday, excluding holidays.

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

If you believe your personal information has been impacted, we recommend that you place an initial one-year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. 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	***Experian***	***TransUnion***
P.O. Box 105069 Atlanta, GA 30348-5069 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (800) 525-6285	P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742	Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016-2000 https://www.transunion.com/fraud-alerts (800) 680-7289

2. Placing a Security Freeze on Your Credit File.

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	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160 Woodlyn, PA 19094

Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/ (888) 298-0045	Allen, TX 75013 http://experian.com/freeze (888) 397-3742	https://www.transunion.com/credit-freeze (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.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If you believe your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take

to protect your account, including whether you should close your account or obtain a new account number.

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.