Union Hill Independent School District
2197 FM 2088 Gilmer, TX 75644
Telephone (903) 762-2140 Fax (903) 762-6845
Dr. Troy Batts, Superintendent

To Parents and Guardians of Union Hill ISD Students:

The Texas Department of Agriculture (TDA) has notified Union Hill ISD of a possible data breach of some student information from a state-issued laptop through a ransomware attack. The specific student's names and information is not known at this time, however, some student information from Union Hill ISD was on the laptop. This was a TDA laptop located in Austin, not an attack on Union Hill ISD nor our equipment. Many schools in the East Texas area were notified of the possible breach.

The purpose of this letter is to make you aware of this possibility, so you can watch for any suspicious activity regarding your student's identity. The breach happened on October 26, 2017 and TDA stated: "The information exposed on the employee's laptop included names, social security numbers, home addresses, birthdates, and personal phone numbers of the affected students and their families." "It is important to note that, to date, TDA's ISO has not discovered any evidence to suggest misuse of the information that was compromised by the ransomware exploit. TDA recognizes the implications of this breach and continually evaluates agency processes and protocols to reduce future occurrences."

Should you have questions about this letter, please contact the school at 903.762.2140. The attached letter is the original correspondence from TDA.

Sincerely,

Dr. Troy Batts

TEXAS DEPARTMENT OF AGRICULTURE
COMMISSIONER SID MILLER

Summary of Ransomware Attack Incident and Recommended Action

On October 26, 2017, a Texas Department of Agriculture (TDA) employee's state-issued laptop computer was compromised through a malicious ransomware attack. As a result, students in school districts throughout Texas may have been potentially impacted by the breach. The information exposed on the employee's laptop included names, social security numbers, home addresses, birthdates, and personal phone numbers of the affected students and their families. To date, TDA's Information Security Officer (ISO) has identified more than 700 students whose sensitive personal information was, or is reasonably believed to have been, exposed to acquisition by an unauthorized person.

It is important to note that, to date, TDA's ISO has not discovered any evidence to suggest misuse of the information that was compromised by the ransomware exploit.

To mitigate this potential exposure, TDA's ISO recommends that the affected students, or parents of the affected students, if minors, contact the three major credit bureaus and activate a fraud alert on behalf of the students impacted by ransomware attack.

Notices are available on TDA's Square Meals website for the children's parents or guardians that are impacted by the ransomware attack. (Section 521.053(f) of the Texas Business and Commerce Code).

Please view list below of affected schools and school districts with students who have been potentially impacted by the successful ransomware.

Independent School Districts Impacted by ransomware attack

ALBA-GOLDEN ISD	KEENE ISD
ALVARADO ISD	KENNEDALE ISD
ARGYLE ISD	KRUM ISD
BIG SANDY ISD-DALLARDSVILLE	LAKE DALLAS ISD
BOLES ISD	MELISSA ISD
BOYD ISD	NECHES ISD
CENTRAL ISD	NEW DIANA ISD
CLEBURNE ISD	ORE CITY ISD
CORISCANA ISD	PARADISE ISD
CROWLEY ISD	PILOT POINT ISD

P.O. BOX 12847
AUSTIN, TEXAS 78711

TEXASAGRICULTURE.GOV

(512) 463-7476
FAX: (888) 223-8861

DALLAS COUNTY JUVENILE DEPARTMENT	PINEYWOODS COMMUNITY ACADEMY
ENNIS ISD	PONDER ISD
ETOILE ISD	PRINCETON ISD
GILMER ISD	SLIDELL ISD
GLADEWATER ISD	ST MARY OF CARMEL SCHOOL
GUNTER ISD	ST GEORGE SCHOOL
HARLETON ISD	TERRELL ISD
HARRISON COUNTY JUVENILE SERVICES	UNION GROVE ISD
JEAN MASSIEU ACADEMY	UNION HILL ISD
KARNACK ISD	

References – Applicable State Law:

Section 521.053(b) of the Texas Business and Commerce Code – requires notice to a person whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Section 521.053(f) of the Texas Business and Commerce Code – authorizes alternate notification via electronic mail, if the person providing notice has electronic mail addresses for the affected persons; conspicuous posting on the entity's website; or broadcast on major statewide media.

Section 521.002(a) of the Texas Business and Commerce Code – defines PII as information that alone or in conjunction with other information identifies an individual, including an individual's name, social security number, date of birth, government-issued identification number, mother's maiden name, personal address, driver's license number, etc.

Worksheet

This worksheet will guide you through the following essential steps to stop fraudulent use of your identity and restore your credit:

- ✓ **Contact the three major credit bureaus**
- ✓ **Contact your creditors**
- ✓ **File a police report and contact the Federal Trade Commission**
- ✓ **Stop payment on stolen checks**

Contact the Fraud Departments at the Three Major Credit Bureaus

Explain that you're a victim of identity theft, and request that a **fraud alert** be placed in your file, as well as a **fraud victim's statement**, which asks creditors to call you before opening any new accounts or making changes to your existing accounts. Be sure to leave a daytime and evening phone number where you can be reached. Also, ask for a free copy of your credit report. Order new copies in a few months to verify that corrections were made and to make sure no new fraudulent activity has occurred.

Bureau	Phone Number	Date Contacted	Contact Person	Comments
Equifax	1-800-525-6285			
Experian	1-888-397-3742			
TransUnion	1-800-680-7289			

Contact Your Creditors

Promptly contact each of your creditors, including, banks, credit card issuers, phone and utility companies, and other lenders. To protect your legal rights, follow-up with a letter to each. Check for fraudulent charges and/or changes-of-address on all your accounts. Close any accounts that have been compromised and open new ones. Be sure to use different, non-obvious Personal Identification Numbers (PINs) and passwords. Ask that inquiries related to fraud be removed.

Creditor	Address/Phone	Date Contacted	Contact Person	Comments

File a Police Report and Contact the Federal Trade Commission

Be sure to file a police report with either your local police or the police department in the community where the theft took place. Get a copy of the report to use as proof of the crime when dealing with creditors. Also file a complaint with the Federal Trade Commission at the number below or via their online ID theft form at https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03. Complaints are entered into a secure consumer fraud database, accessible only to law enforcement agencies, for use in pursuing criminal investigations.

Agency/ Department	Phone Number	Date Contacted	Contact Person	Report # and Comments
Federal Trade Commission	1-877-IDTHEFT (438-4338)			
Local Police				

Stop Payment on Stolen Checks

If your checks have been stolen or misused, contact your bank immediately to obtain stop payment instructions. Also contact the major check verification companies below to request that they notify retailers using their databases not to accept these checks. If your ATM/debit card has been lost, stolen or otherwise compromised, cancel the card as soon you can get a new PIN.

Institution	Phone Number	Date Contacted	Contact Person	Comments
Your Bank				
Certegy, Inc	1-800-437-5120			
Global Payments	1-800-766-2748			
TeleCheck	1-800-710-9898			
SCAN	1-800-262-7771			

Additional Needs of Identity Theft Victims

Issue	Contact
Remove fraudulent phone charges (within your state)	State Public Utility Commission
Remove fraudulent long distance or cellular phone charges	1-888-CALL-FCC (1-888-225-5322)
Report fraudulent use of your Social Security Number	1-800-772-1213
Report misuse of your name or Social Security Number to get a drivers license	State Dept of Motor Vehicles or via www.onlinedmv.com
Report your mail has been stolen and used to obtain new accounts	U.S. Postal Inspector - www.usps.gov/websites/depart/inspect or your local phone directory