IMPORTANT SECURITY AND PERSONAL DATA PROTECTION NOTIFICATION

March 5, 2019

The Thomas County School District values its employees and wants you to be aware of an incident that may involve your bank account information. We recently became aware of a breach of our online banking system. After discovering the issue, we immediately engaged BlueVoyant, a leading IT investigation and security firm, to determine the facts. Protecting the security of our employees' personal information is a top priority for the District. We value and respect the privacy of your information, and we sincerely apologize for any concern or inconvenience this may cause you.

What Happened?

The District was recently the target of malicious cyber activity. Criminals obtained unauthorized access to a computer with banking information stored on it, including employee payroll information. The employee payroll information included the names, employee ID numbers **(not Social Security numbers)**, bank account numbers, and bank routing numbers for District employees. Soon after discovering the potential breach, the District retained BlueVoyant to deploy specialized software to prevent further attacks.

We are still conducting our investigation into the scope of this attack. We wanted to alert you of these facts so you can make informed choices about your use of your bank accounts and how best to protect yourself from potential fraud associated with any unauthorized access to your bank account information.

When Did This Happen?

Our investigation to date has revealed the breach may have occurred beginning around February 7, 2019. The breach may have continued for several days after.

What Information Was Involved?

Based on the facts known to the District at this time, the criminals sought to infiltrate the District's banking system in an effort to transfer money from District accounts to the criminals' accounts. It appears at this time their primary objective was the theft of District funds. Fortunately, the fraudulent transfers were prevented by certain control processes maintained by our banking relationship and no money was lost.

What Are We Doing?

Shortly after learning of the intrusion, we engaged BlueVoyant to determine the facts and contain the intrusion and commenced remediation procedures. We have deployed additional IT security measures to reduce risk of further attacks. The District has and continues to work aggressively with BlueVoyant on this investigation, which is ongoing.

How Does This Incident Affect Me?

Even if you receive this notice, it does not mean you will be affected by this issue. Out of an abundance of caution, you may want to review and monitor the statements and activity of the bank account into which your paycheck is deposited. If you believe your account may have been affected, please contact your bank immediately.

What can I do to help prevent unauthorized access to my computer and email account?

We recommend that you change your password on your District computer. To change the password in a Windows Operating System, simply press CTRL-ALT-DEL simultaneously at your desktop screen. The screen will overlay a menu and one of the selections will be "Change a Password". Select this item and follow the directions. Changing this password will also change your Google, Infinite Campus, Clever, and Sherpadesk passwords immediately. If you have any questions, please contact your school technology specialist or digital learning specialist.

If you receive an unexpected email that appears to be from a colleague, **think before you click**. If you have any doubts about an email's authenticity, do not hesitate to contact the sender and send it to your school technology specialist.

If you receive a prompt that asks you to sign in again after opening an attachment, **stop**! The email is probably a phishing attempt. Contact your school technology specialist immediately to confirm any sign-in prompts.

Look for possible red flags:

1. Does the sender ask you to click on a link or open an attachment? If yes, why?
2. Does the sender typically send you this type of email?
3. Is the language in the email vague, or are relevant details included in the subject line and body of the email? For example, the Human Resources, Finance, and Technology departments always include details and specifics about the purpose of the emails they send.
4. Does the email have grammar or spelling mistakes?

If you are not sure if the email is legitimate, do not click the link or open the attachment. Call your colleague to confirm if the email is legitimate and contact your school technology specialist.

What Else Can I Do to Protect My Information?

We recommend that you remain vigilant, review your relevant account statements, and monitor your credit reports for suspicious activity. Some state laws advise you to report any suspected identity theft to law enforcement, your state's Attorney General, and the Federal Trade Commission. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740241 Atlanta, Georgia 30348 www.equifax.com	Phone: 888-397-3742 P.O. Box 9532 Allen, Texas 75013 www.experian.com	Phone: 800-680-7289 P.O. Box 6790 Fullerton, CA 92834 www.transunion.com

Fraud Alerts: At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This can be done by contacting the credit bureaus by phone and also via Experian's or Equifax's website. Once you place a fraud alert at one credit bureau, that bureau is required to notify the other two and have alerts placed on your behalf. Note, however, that because the alert tells creditors to follow certain procedures to protect you, it may also delay your efforts to obtain credit while the agency verifies your identity.

Security Freezes: You have the right to place a security freeze on your credit report. A security freeze is intended to prohibit a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail in order for the freeze to be effective. In order to request a security freeze, you will need to provide the following information: (1) full name (including middle initial and any suffixes); (2) Social Security number; (3) date of birth; (4) current address and previous addresses for the past five years; (5) proof of current address, such as a current utility bill, bank statement, or insurance statement; (6) a legible photocopy of a government issued identification card (state driver's license, military identification, etc.); (7) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze.

You may also place a security freeze on your credit report online by visiting the below links:

https://www.experian.com/freeze/center.html
https://www.transunion.com/credit-freeze
https://www.equifax.com/personal/credit-report-services/

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit www.identitytheft.gov or call 1-877-ID-THEFT

(877-438-4338). IdentityTheft.gov is the federal government's one-stop resource for identity theft victims. The site provides streamlined checklists and sample letters to guide you through the recovery process.

Who Can I Contact?

For any additional questions or information, including as to the breach and the information potentially compromised, please contact:

Joey Holland – 229-224-2051 (cell)

Dusty Kornegay – 229-221-5025 (cell)

Brecca Pope – 229-221-0804 (cell)

Frequently Asked Questions

When did the District first discover the data breach?

Our investigation to date has revealed the breach may have occurred beginning around February 7, 2019. The breach may have continued for several days after.

What type of personal information was exposed in the data breach?

Employee payroll information, including names, employee ID numbers (**not** Social Security numbers), bank account numbers, and bank routing numbers.

What happened?

Based on the facts known to the District at this time, the criminals sought to infiltrate the District's banking system in an effort to transfer money from district accounts to the criminals' accounts. It appears at this time their primary objective was the theft of District funds. Fortunately, the fraudulent transfers were prevented by certain control processes maintained by our banking relationship, and no money was lost.

How did the criminals get into the District's system?

Criminals obtained unauthorized access to a computer with banking information stored on it, including employee payroll information. The employee payroll information included the names, employee ID numbers **(not Social Security numbers)**, bank account numbers, and bank routing numbers for District employees.

What can I do now to protect myself and my personal information?

You may wish to contact your credit card(s), bank(s), and/or other financial companies you have relationships with to alert them that your identity may have been compromised and to establish additional security on your personal accounts. You should also monitor your credit report. You should follow the steps outlined in the notice, including alerting law enforcement, if you detect any fraudulent activity on your payment card or other accounts.

Who at the District can I speak with about the data breach?

If you have questions, concerns or suggestions, please contact Joey Holland (229-224-2051), Dusty Kornegay (229-221-5025), or Brecca Pope (229-221-0804).

What steps will the District take in the future to protect my personal information?

The District is consulting with legal and information security experts to review all security processes and procedures. At this time, the District has taken measures to prevent further unauthorized access to its accounting and banking systems. The District has an ongoing commitment to enhancing its overall security architecture and processes including but not limited

to the establishment of a more robust and mandatory security awareness program, revamped policies to minimize personally identifiable information accepted through email, and implementation of routine mandatory password changes.

How do I re-set my password on my District computer? Is this an automated process or do I have to call?

The process to change your password on your District computer is automated. To change the password in a Windows Operating System simply press CTRL-ALT-DEL simultaneously at your desktop screen. The screen will overlay a menu and one of the selections will be "Change a Password". Select this item and follow the directions. **Note that changing this password will also change your Google, Infinite Campus, Clever, and Sherpadesk passwords immediately.** If you have any questions, please contact your school technology specialist or digital learning specialist.

What is a Data Breach?

A data breach is an incident in which sensitive, protected, or confidential data has been potentially viewed by an individual unauthorized to do so.

What is Identity Theft?

Identity theft is a crime in which an imposter obtains key pieces of personal information, such as a financial account number, in order to impersonate someone else.

What is the difference between a Data Breach and Identity Theft?

A Data Breach means that someone has access to your data.

Identity Theft is the usage of this data to commit theft.

Not all Data Breaches result in Identity Theft. According to government and law enforcement, many stolen records are difficult to use successfully.

What is a fraud alert?

A fraud alert on your credit report notifies lenders and creditors who pull your report to take additional steps to verify your identification before they extend a credit line or loan in your name. You may place a free 90-day fraud alert on your credit report with any of the three major credit bureaus, namely Equifax, Experian and TransUnion. Once you place an alert with one of the three agencies it is shared with the other two agencies. You do not need to contact all three agencies.

Can I place a seven-year fraud alert?

In order to place a seven-year fraud alert you must personally be a victim of fraud or identity theft and must, as an individual, file a police report. You can then use this police report to add a seven-year fraud victim alert to your credit report.

What is the difference between a Credit Freeze and a Fraud Alert on my Credit Report?

A credit freeze locks down your credit. A fraud alert allows creditors to get a copy of your credit report as long as they take steps to verify your identity. For example, if you provide a telephone number, the business must call you to verify whether you are the person making the credit request. Fraud alerts may be effective at stopping someone from opening new credit accounts in your name, but they may not prevent the misuse of your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

Should I put a Credit Freeze on my Credit Report?

No, you need not put a credit freeze on your credit report.

A credit freeze generally stops all access to your credit report, and it will essentially lock down your credit, while a fraud alert permits creditors to get your report as long as they take steps to verify your identity.

A credit freeze may not stop misuse of your existing accounts or some other types of identity theft. Also, companies that you do business with would still have access to your credit report for some purposes. A fraud alert will allow some creditors to get your report as long as they verify your identity.

The availability of a credit freeze depends on state law or a consumer reporting company's policies; fraud alerts are federal rights intended for people who believe they are, or who actually have been, identity theft victims.

Some states charge a fee for placing or removing a credit freeze, but it's free to place or remove a fraud alert.