



Jason Cherry, Partner
Cybersecurity & Data Privacy Team
2029 Century Park East
Los Angeles, CA 90067
Telephone: 207.745.1397

November 15, 2024

VIA ELECTRONIC MAIL

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

Re: Notice of Data Security Incident

To Whom it May Concern:

Constangy, Brooks, Smith & Prophete, LLP (“Constangy”) represents Abilene Independent School District (“AISD”), a public school district in Texas, in connection with a data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland’s data breach notification statute.

1. Nature of the Security Incident

On June 9, 2024, AISD experienced a network disruption. AISD immediately took steps to secure its network environment and engaged cybersecurity experts to conduct an investigation to determine what happened. The investigation conducted by the third-party cybersecurity experts determined that an unknown actor accessed and acquired certain data without authorization. AISD then worked with additional experts to conduct a comprehensive review of the affected data to determine whether personal information may have been affected. This process was completed on October 17, 2024.

2. Number of Affected Maryland Residents & Information Involved

On November 15, 2024, AISD notified seven (7) Maryland residents. The information involved in the incident for the affected Maryland residents may have included name and Social Security number.

3. Notification of Affected Individuals

On November 15, 2024, a notification letter was mailed to the affected Maryland residents by USPS First Class Mail. The notification letter provides resources and steps the individuals can take to help protect their information. The notification letter also offers the opportunity to enroll in (twelve) 12 months of complimentary identity protection services, including credit monitoring, identity protection services and a call center through Epiq, a company specializing in fraud assistance and remediation services. A sample notification letter sent to the impacted individuals is included with this correspondence.

November 15, 2024

Page 2

4. Steps Taken to Address the Incident

In response to the incident, AISD retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. AISD also implemented additional security measures to further harden its digital environment in an effort to prevent a similar event from occurring in the future. Finally, AISD is notifying the affected individuals and providing them with steps they can take to protect their personal information as discussed above.

5. Contact Information

AISD remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at jcherry@constangy.com or 207.745.1397.

Sincerely,

A handwritten signature in blue ink, appearing to read "Jason S. Cherry".

Jason Cherry of
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Consumer Notification Letter



Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

Subject: <<Notice of Data Security Incident/Data Security Breach>>

Dear <<Full Name>>:

We are writing to inform you of a data security incident that may have involved your personal information. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information.

What Happened? On June 9, 2024, Abilene Independent School District (“AISD”) experienced a network disruption. We immediately took steps to secure our network environment and engaged cybersecurity experts to conduct an investigation to determine what happened. The investigation determined that certain files may have been acquired without authorization. We then conducted a comprehensive review of the affected data to determine whether personal information may have been involved. After a thorough review of the impacted data, on October 17, 2024, it was determined that some of your personal information was present in the data set. We then took steps to notify you of the incident as quickly as possible. We do not have any evidence that personal information was misused, and our notification timeline is in compliance with applicable laws and was sensitive to the ongoing investigation.

What Information Was Involved? The information involved may include your name and <<Breached Elements>>.

What We Are Doing. As soon as we discovered the incident, we took the steps described above. We also implemented additional measures to reduce the risk of a similar incident occurring in the future.

We are also offering you the ability to enroll in <<12/24>> months of complimentary Equifax Credit Watch Gold credit monitoring and identity protection services through Equifax, a global technology services leader.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the Equifax Credit Watch Gold identity protection services, which are offered at no cost to you.

To enroll in Equifax Credit Watch Gold visit www.equifax.com/activate

Enter your unique Activation Code of <<ACTIVATION CODE>> then click “Submit” and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click 'Sign Me Up' to finish enrolling.

You're done!

The confirmation page shows your completed enrollment.

Click "View My Product" to access the product features.

Please note the deadline to enroll in these complimentary services is <<Enrollment Deadline>>. Please do not discard this letter, as you will need the Activation code provided above to access services.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 855-278-0537, Monday through Friday, 8:00 AM to 8:00 PM Central time. Epiq representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

We take your trust in us and this matter very seriously. We deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Abilene Independent School District
241 Pine Street
Abilene, TX 79601

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the “FTC”).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

Federal Trade Commission: Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.