



Donna Maddux
4800 Meadows Road, Suite 300
Lake Oswego, OR 97035
dmaddux@constangy.com
Direct: 503.312.6251

June 14, 2023

VIA EMAIL

Attorney General Brian E. Frosh
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Fax: (410) 576-6566

Re: Notice of Data Security Incident

Dear Office of the Attorney General:

Constangy, Brooks, Smith & Prophete LLP ("Constangy") represents Dallas School District #2. ("DSD"), a school district based in Dallas, Oregon, in conjunction with the recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with the Maryland data breach notification statute.

1. Nature of the Security Incident

On January 27, 2023, DSD discovered unusual network activity that disrupted access to certain systems. Upon discovering this activity, DSD immediately took steps to secure its network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened and whether sensitive information may have been affected. As a result of this investigation, DSD learned certain personal information may have been acquired without authorization during the incident. On or about May 31, 2023, DSD completed a comprehensive review of the impacted data potentially containing personal information through which DSD identified certain personal information as potentially involved. DSD then worked diligently to identify current contact information to issue notification to relevant individuals.

2. Type of Information and Number of Maryland Residents Notified

The data sets potentially acquired by the malicious actor(s) responsible for this incident included individuals' names, Social Security numbers, dates of birth, medical information, health insurance information, payment card information or student identification numbers. On June 14, 2023, DSD notified one (1) Maryland resident of this data security incident via U.S. First-Class Mail. This one (1) resident of Maryland was an adult. A sample copy of the notification letter sent to potentially impacted individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

Alabama California Colorado Florida Georgia Illinois Massachusetts Minnesota Missouri
New Jersey New York North Carolina South Carolina Tennessee Texas Virginia

DSD reported this incident to federal law enforcement and will cooperate with investigative requests as necessary. It has also implemented additional security measures in an effort to prevent a similar incident from occurring in the future. Further, as referenced in the sample consumer notification letter, DSD has offered individuals 12 months of complimentary services through IDX, which include credit monitoring, dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully-managed identity theft recovery services, along with access to a call center for support for 90 days.

4. Contact Information

DSD remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at dmaddux@constangy.com.

Best regards,

Very truly yours,

/s/ Donna Maddux

Donna Maddux of
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Encl: Sample Adult Consumer Notification Letter



Return Mail to IDX:
4145 SW Watson Avenue
Suite 400
Beaverton, OR 97005

To Enroll, Please Call:

1-800-939-4170

Or Visit:

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

Enrollment Code: <<XXXXXXXX>>

<<First Name>> << Last Name>>

<<Address1>>

<<Address2>>

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

June 14, 2023

Subject: Notice of Data <<Variable Text 2>>

Dear <<First Name>> << Last Name>>:

Dallas School District #2 (“DSD”) is writing to inform you of a recent data security incident that may have involved your personal information. DSD takes the privacy and security of all information within its possession very seriously. We are writing to notify you about the incident, provide you with information about steps you can take to help protect your personal information, and offer you the opportunity to enroll in complimentary identity protection services that DSD is making available to you.

What Happened? On January 27, 2023, DSD discovered unusual network activity that disrupted access to certain systems. Upon discovering this activity, DSD immediately took steps to secure our network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened and whether sensitive information may have been affected. The investigation subsequently revealed that certain personal information may have been accessed or acquired without authorization during the incident. On or about May 31, 2023, we completed a comprehensive review of the impacted data potentially containing personal information which identified your information as potentially involved. We then took steps to notify you of the incident as quickly as possible. <<Variable Text 3>>.

What Information Was Involved? The information that may have been impacted includes your name and <<Variable Text 1>>.

What Are We Doing? As soon as we discovered this incident, we took the steps described above. In addition, we reported this incident to federal law enforcement and will cooperate with investigative requests as necessary. We also implemented additional security measures to help reduce the risk of a similar incident occurring in the future. We are further notifying you of this event and advising you about steps you can take to help protect your information.

In addition, we are offering you the opportunity to enroll in complimentary identity protection services through IDX – a data breach and recovery services expert. These services include <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. Please note that the deadline to enroll in these services is September 14, 2023.

What Can You Do? DSD recommends that you review the guidance included with this letter about how to protect your information. You can also enroll in the complimentary identity protection services being offered to you by using the Enrollment Code provided above.

For More Information: Further information about how to help protect your information appears on the following page. If you have questions about this matter or need assistance enrolling in the complimentary services being offered to you, please call IDX at 1-800-939-4170 from 6:00 A.M. to 6:00 P.M. Pacific Time, Monday through Friday (excluding holidays).

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Steve Spencer

Steve Spencer
Superintendent
Dallas School District #2

STEPS YOU CAN TAKE TO HELP PROTECT YOUR 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 (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 <http://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 <http://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.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

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 <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.