Donna Maddux, Partner
Cybersecurity & Data Privacy Team
4800 SW Meadows Road, Suite 300
Lake Oswego, Oregon 97035
Telephone: 503.312.6251
Email: dmaddux@constangy.com

June 23, 2023

VIA ELECTRONIC MAIL

Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: **Notice of Data Security Incident – Supplemental Notice to Initial Notice Submitted February 24, 2023.**

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP ("Constangy") represents David Douglas School District ("DDSD"), a school district in Portland, Oregon, in connection with a recent data security incident described in greater detail below. We are writing to provide an update with respect to additional New Hampshire residents that DDSD notified of the incident after having completed its review of potentially affected information.

Nature of the Security Incident

On January 29, 2023, an unknown individual burglarized a DDSD office and stole a number of electronic devices, including a physical hard drive. DDSD initiated an investigation into the contents of the hard drive and took steps to identify personal information contained therein, including the engagement of an independent team to perform a comprehensive review of all data contained on the hard drive. While the full review was ongoing, on February 24, 2023, DDSD notified one (1) New Hampshire resident it believed to have information stored on the hard drive.

On May 1, 2023, the comprehensive review identified that the personal information related to additional current and former DDSD employees was stored on the stolen hard drive. DDSD then worked diligently to obtain missing addresses to effectuate notification, which was completed on June 10, 2023.

The information affected may have included . Please note that we have no current evidence to suggest misuse or attempted misuse of personal information stored on the hard drive.

Number of New Hampshire Residents Involved

On June 21, 2023, DDSD notified an additional five (5) New Hampshire residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence. In combination with the one (1) resident notified on February 24, 2023, a combined total of six (6) New Hampshire residents have been notified of the incident.

Steps Taken to Address the Incident

To help reduce the risk of a similar future incident, DDSD has implemented additional physical security measures on its campus. Additionally, DDSD has reported the incident to the Portland Police Bureau and will cooperate with any resulting investigation.

DDSD is also providing the identified employees with information about steps that they can take to help protect their personal information and is offering complimentary credit monitoring and identity protection services through IDX. For New Hampshire residents, these services include of credit monitoring and CyberScan dark web monitoring, a $1,000,000 identity fraud loss reimbursement policy, and fully managed identity theft recovery services.

Contact Information

DDSD 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 .

Sincerely

Donna Maddux of
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Consumer Notification Letter

DAVID DOUGLAS SCHOOL DISTRICT
Learn • Grow • Thrive

P.O. Box 1907
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

June 21, 2023

Re: Notice of Data <<Variable Text 1>>

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a recent data security incident experienced by David Douglas School District ("DDSD") that may have involved your personal information. At DDSD, we take the privacy and security of all information within our possession very seriously. This is why we are notifying you of the incident, providing you with steps you can take to help protect your personal information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened? On January 29, 2023, an unknown individual burglarized a DDSD office and stole a number of electronic devices, including a physical hard drive. DDSD immediately initiated an investigation into the contents of the hard drive and took steps to identify any personal information contained on the stolen hard drive, including the engagement of an independent team to perform a comprehensive review of all data on the hard drive. On May 1, 2023, this review identified that the personal information related to specific current and former DDSD employees was stored on the stolen hard drive. DDSD then worked diligently to obtain missing addresses for potentially affected individuals to effectuate notification, which was completed on June 10, 2023.

At this time, we have no reason to believe the personal information of DDSD students was involved in the incident. Please note that we have no current evidence to suggest access to or the misuse or attempted misuse of the personal information stored on the hard drive.

What Information Was Involved? The information stored on the hard drive may have included , <<Variable Text 2 – Data Elements >>.

What We Are Doing. As soon as DDSD learned of the incident, we took the measures described above. We also implemented additional security features to reduce the risk of a similar incident occurring in the future. Furthermore, we reported the incident to the Portland Police Bureau and will provide whatever cooperation is necessary to hold the perpetrator(s) accountable, if possible. We are also providing you with information about steps you can take to help protect your personal information.

Additionally, we are offering you the opportunity to enroll in credit monitoring and identity protection services through IDX, at no cost to you. The IDX services, which are free to you upon enrollment, include of credit monitoring and CyberScan dark web monitoring, a $1,000,000 identity fraud loss reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you to resolve issues if your identity is compromised.

What You Can Do. Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information. In addition, we encourage you to enroll in the credit monitoring and identity theft protection services we are offering through IDX at no cost to you. To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

You can enroll in the IDX identity protection services by calling
and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time. Please note the deadline to enroll is September 21, 2023.

For More Information. If you have questions, please call IDX at , Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time. IDX representatives are fully versed on this incident and can answer questions you may have regarding the protection of your personal information.

Please accept our sincere apologies and know that we deeply regret any concern or inconvenience that this may cause you.

Sincerely,

Patt Komar
Director of Administrative Services
David Douglas School District
11300 NE Halsey St.
Portland, OR 97220

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER 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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *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.

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 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 can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 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 Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. 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. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov

California: California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; http://oag.ca.gov/

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; https://www.maine.gov/ag/

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; https://ag.ny.gov/

Oregon: Oregon Office of the Attorney General can be reached at: Oregon Department of Justice, 1162 Court St. NE, Salem, OR, 97301, 1-877-877-9392, www.doj.state.or.us

Rhode Island: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, http://www.riag.ri.gov. The total number of Rhode Island residents receiving notification of this incident is XX.

Texas: Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov