November 29, 2021

Broward County Public Schools
Notice of Compromised Data Resulting from Security Incident

This notice is to inform you that the March 7, 2021 security incident that resulted in unauthorized access to some Broward County Public Schools ("BCPS" or "the District") systems may have potentially included the sensitive information of some faculty, staff, and students.

Through an investigation, it was determined that an unauthorized person obtained access to BCPS systems between November 12, 2020, and March 6, 2021. On April 19, 2021, the investigation revealed certain records stored on the District's systems had been acquired and publicly released. On June 8, 2021, it was determined that the records released by the cyber criminals included information that included individuals' names and Social Security numbers. On June 29, 2021, further analysis indicated that the data accessed may include information relating to our self-insured health plan, including individuals' names, dates of birth, Social Security numbers, and benefits selection information.

The District is now providing written notification to the affected individuals. In an abundance of caution, BCPS is also posting this notice to inform the public (including all those who did not receive a written notification from the District) about the extent of this incident and provide recommendations on ways to protect personal information. The District is also offering complimentary credit monitoring, by request, to those affected.

The District has established a dedicated call center for anyone who has questions about the incident. If you have any questions, call 1-855-545-1943, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Standard Time, excluding some U.S. holidays.

To further protect personal information, the District has implemented additional measures to enhance the security of its network.

You are encouraged to remain vigilant by reviewing your accounts statements, health provider invoices, explanation of benefits statements and free credit reports for any unauthorized activity. If you notice any unauthorized activity, you should immediately contact the relevant financial institution, healthcare provider or credit bureau reporting the activity. In addition, please see below for additional steps you can take to protect your personal information.

ADDITIONAL STEPS YOU CAN TAKE

We encourage you to remain vigilant by reviewing your accounts statements, health provider invoices, explanation of benefits statements and free credit reports for any unauthorized activity. If you notice any unauthorized activity, you should contact the relevant financial institution, healthcare provider or credit bureau reporting the activity immediately.

You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. 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 Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

If your health insurance or medical information was involved, it is also advisable to review the billing statements you receive from your health insurer or healthcare provider. If you see charges for services you did not receive, please contact the insurer or provider immediately.

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.
To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
- TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com
- Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a 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 by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.