CUMMINS
Behavioral Health Systems, Inc.
P.O. Box 989728
West Sacramento, CA 95798-9728

Via First-Class Mail

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/
CumminsBehavioralHealthSystems

August 11, 2023

Notice of Data <<Variable Text 3>>

Dear <<FIRST NAME>> <<LAST NAME>>:

Cummins Behavioral Health Systems, Inc. recently experienced a data security incident which may have affected your personal information. Based on our current review, we have no indication that your personal information has been or will be used inappropriately, but we wanted to make you aware of the incident, the measures we have taken in response, and to provide details on the proactive steps you can take to help protect your information. We take the protection and proper use of personal information seriously and are working to prevent a similar incident from occurring again in the future. <<CA Residents: This notification was not delayed by law enforcement.>>

What Happened

On or about March 9, 2023, Cummins Behavioral Health Systems, Inc. discovered a ransom note within its environment, placed by an unathorized individual. During a typical ransomware incident, cybercriminals try to encrypt or "lock" an organization's digital files in an attempt to get paid for a digital key to unlock the files. Significantly, no encryption occurred as a result of the incident. We promptly launched an investigation, engaged a national cybersecurity firm to assist in assessing the scope of the incident and took steps to mitigate the potential impact to our community. Unfortunately, these types of incidents are becoming increasingly common and even organizations with some of the most sophisticated IT infrastructure available are affected. We have worked diligently to determine what happened and what information was involved as a result of this incident. A third-party forensic investigation determined the incident occurred between February 2, 2023 and March 9, 2023. <<RI Residents: The forensic investigation further determined that the incident potentially impacted approximately <<written number>> (<<#>>) Rhode Island residents.>>

What Information Was Involved

The elements of your personal information that may have been impacted may have included, and potentially were not limited to, your: name, <<PII data elements>> <<PHI data elements>>. Please note that there is no evidence at this time that any of your personal information has been or will be misused as a result of the incident.

What We Are Doing

We are taking this incident seriously and are committed to strengthening our systems' security to prevent a similar event

from occurring again in the future. Additionally, out of an abundance of caution, we have arranged for you to enroll in a complimentary, credit monitoring and identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<twelve (12)/twenty-four (24)>> months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

To enroll in the complimentary credit monitoring service that we are offering you, please go to https://response.idx.us/CumminsBehavioralHealthSystems and using the Enrollment Code provided above, follow the steps to receive the credit monitoring service online within minutes. If you do not have access to the Internet and wish to enroll, please call IDX's toll-free hotline at 1-888-756-0010.

You can sign up for the credit monitoring service anytime between now and November 11, 2023. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain <<twelve (12)/twenty-four (24)>> months of credit monitoring service which will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

At this time, we are not aware of anyone experiencing fraud as a result of this incident. As data incidents are increasingly common, we encourage you to always remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. Additionally, we recommend that you review the following page, which contains important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes.

For More Information

Please know that the protection of your personal information is a top priority, and we understand the inconvenience and concern his incident may cause. If you have any questions, please do not hesitate to call 1-888-756-0010, available Monday through Friday, between the hours of 9:00 a.m. and 9:00 p.m. Eastern Time.

Sincerely,

Cummins Behavioral Health Systems, Inc.

Additional Important Information

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian_(https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
equifax.com/personal/credit-report-services/
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
transunion.com/credit-freeze
1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.

Implementing an Identity Protection PIN (IP PIN) with the IRS:
To help protect against a fraudulent tax return being filed under your name, we recommend Implementing an Identity Protection PIN (IP PIN) with the IRS. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account.

If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft. If you want to request an IP PIN, please note: you must pass an identity verification process; and Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool found at: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. If you wish to get an IP PIN and you don't already have an account on IRS.gov, you must register to validate your identity.

Some items to consider when obtaining an IP PIN with the IRS:

- An IP PIN is valid for one calendar year.
- A new IP PIN is generated each year for your account.
- Logging back into the Get an IP PIN tool, will display your current IP PIN.
- An IP PIN must be used when filing any federal tax returns during the year including prior year returns.

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Vermont*: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

For residents of *New Mexico*: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For Residents of *Washington, D.C.*: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of *Massachusetts and Rhode Island*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.