McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

Colin M. Battersby
Direct Dial: 248-593-2952
E-mail: cbattersby@mcdonaldhopkins.com

May 17, 2023

VIA U.S. MAIL

Office of the Attorney General
700 W. Jefferson Street, Suite 210
P.O. Box 83720
Boise, ID 83720-0010

Re: Brightline, Inc. – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Brightline, Inc. ("Brightline"). I am writing to provide notification of an incident involving Fortra (formerly known as HelpSystems), Brightline's vendor, that may have affected the security of personal information of approximately six (6) Idaho residents, as discussed in further detail below. Brightline is providing this notification on behalf of certain other entities identified in the enclosed addendum that provided Brightline with the data impacted in this incident. To date, Fortra has refused to provide notice to individuals or regulators on Brightline's behalf, despite repeated requests. By providing this notice, Brightline and the listed entities do not waive any rights or defenses, including but not limited to regarding the applicability of Idaho law or personal jurisdiction.

Fortra is a third-party provider of file transfer services known as GoAnywhere MFT Software-as-a-Service ("SaaS"). On February 4, 2023, Fortra informed Brightline that it was made aware on January 30, 2023 of suspicious activity within certain instances of its GoAnywhere MFT SaaS. Though we understand its investigation is ongoing, Fortra states that it identified a previously-unknown vulnerability which an unauthorized party used to access certain GoAnywhere customers' accounts and download files. Fortra represented that, through its investigation, it identified unauthorized access to and acquisition of data from certain customers' accounts, including Brightline's. Fortra also indicated that it promptly notified law enforcement and is cooperating with their investigation of the incident. We understand that the Fortra GoAnywhere MFT SaaS security incident affected multiple organizations and businesses, including those in the medical sector.

Immediately upon learning of the incident from Fortra, Brightline engaged its incident response plan and confirmed that the unauthorized access was terminated. Brightline took swift action the same day in response to the notice by confirming Fortra deactivated the unauthorized

user's credentials, disabling the vulnerable java servlet, and rebuilding Brightline's instance on new infrastructure. Further, Brightline implemented additional security measures, including a whitelisting for limited IP addresses to access the previously vulnerable administrative portal, removal of all Brightline data from the GoAnywhere MFT SaaS, and ongoing measures to reduce data exposure until an alternative file transfer solution is identified and implemented. Additionally, Brightline retained cyber counsel to assist with its investigation. Brightline's investigation determined the incident was limited solely to the GoAnywhere MFT SaaS.

Subsequently, Brightline determined that the unauthorized party acquired certain files that were saved in the GoAnywhere MFT SaaS. After making this determination, Brightline immediately began to analyze the files to determine which individuals and data had been affected. Brightline determined that the information exposed in the incident involved the affected residents' names, addresses, member IDs, dates of birth, phone numbers, employer names and their group ID numbers, and coverage start/end dates.

To date, Brightline is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, Brightline wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Brightline is providing the affected residents with written notification of this incident commencing on or about April 7, 2023 in substantially the same form as the letter attached hereto. Brightline is offering the affected residents complimentary two-year memberships with a credit monitoring service. Brightline is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission. In addition, the company has established a call center to answer consumer questions.

At Brightline, protecting the privacy of personal information is a top priority. While Brightline's investigation has determined that the incident was limited solely to Fortra's GoAnywhere MFT SaaS, Brightline continues to enhance its cybersecurity program to further safeguard its systems from cyber threats.

Should you have any questions concerning this notification, please contact me at (248) 593-2952 or cbattersby@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

Colin M. Battersby

Encl.

IMPACTED ENTITIES

EXL Service.com, LLC, 6

Brightline, Inc.

[redacted]

[redacted]

April 7, 2023

0000010103G0400

P

NOTICE OF DATA BREACH

Re: **Important Security Notification**
Please read this letter.

Dear [redacted],

Brightline, a virtual behavioral health provider, is writing to inform you about a data security incident that affected some of your personal information. You are covered under a group health plan offered through [redacted] and serviced by [redacted] which includes the offering of Brightline as an in-network provider. Your information was affected even if you have never used Brightline's services because this incident affected eligibility information shared with Brightline for administrative purposes.

The incident involved Fortra, a third-party provider of file transfer services known as GoAnywhere MFT Software-as-a-Service. We understand that the GoAnywhere MFT security incident affected multiple organizations and businesses, including those in the medical sector.

The parties involved value your relationship and respect the privacy of your family's personal information. We want you to understand the steps we have taken to address this issue and additional steps you can take to protect the personal information of yourself. The remaining sections of this letter explain the incident and offer additional assistance for protecting your information, including complimentary identity theft protection and credit monitoring services.

What Happened: While Fortra's investigation is ongoing, we understand that on January 30, 2023, Fortra was made aware of suspicious activity within certain instances of its GoAnywhere MFT service. Through its investigation, Fortra states that it identified a previously-unknown vulnerability which an unauthorized party used to gain access to certain Fortra customers' accounts and download files.

Fortra informed customers, including Brightline, about the security vulnerability in their GoAnywhere MFT service on February 4, 2023. We took swift action the same day in response to the notice. Our investigation determined the incident was limited solely to the Fortra service and did not impact Brightline's network. Fortra also promptly notified law enforcement and is cooperating with their investigation of the Fortra incident.

Subsequently, we determined that the unauthorized party acquired certain files that were saved in the Fortra service. After making this determination, we immediately began to analyze the files to determine which individuals and data had been affected. As part of that analysis, it was determined that those files contained some of your personal information. Your employer was notified of this incident by Aetna on or around the 15th of March, and we have been working with them since.

What Information Was Involved: Based on the investigation, we identified personal information for you in the files that the unauthorized party acquired, including the following data elements: your name, your address, your member ID, your date of birth, your phone number, your employer's name and their group ID number, and your coverage start/end dates.

It is important to note that no Social Security Numbers or financial accounts were included, nor did the files contain anything related to medical services, conditions, diagnoses, or claims for you. The files were to be used for eligibility verification as well as potential outreach, which is why the information included was largely demographic in nature. This means that your information was affected even if you have never used Brightline's services.

What We Are Doing: As soon as we became aware of the incident, we took immediate action to investigate it by confirming Fortra deactivated the unauthorized user's credentials, turned off the service and rebuilt Brightline's version so it was no longer vulnerable. Further, we implemented additional security measures, including limiting ongoing access to verified users, removing all Brightline data from the service, and continuing ongoing measures to reduce data exposure until an alternative file transfer solution is identified and implemented. Additionally, we retained cyber counsel to assist with our investigation. While our investigation has determined that the incident did not impact our systems directly, we continue to enhance our cybersecurity program to further safeguard from cyber threats.

As a precaution, we have secured the services of Cyberscout to provide identity theft restoration and credit monitoring services at no cost to you for 2 years.

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring / Single Bureau Credit Report / Single Bureau Credit Score** services at no charge. These services provide you with alerts for 2 years from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How To Enroll For Free Services: To enroll in Credit Monitoring services at no charge, please log on to [redacted] and follow the instructions provided. When prompted please provide the following unique code to receive services: 4[redacted]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do:

Order Your Free Credit Report. To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's (FTC) website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

The three credit bureaus (Equifax, Experian, and TransUnion) provide free annual credit reports only through the website, toll-free number, or request form. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax www.equifax.com	(800) 685-1111
Experian www.experian.com	(888) 397-3742
TransUnion www.transunion.com	(800) 916-8800

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Upon receiving your credit report, review it carefully. Errors may be a warning sign of possible identity theft. Here are a few tips of what to look for:

- Look for accounts you did not open.
- Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case.
- Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

Federal Trade Commission and State Attorneys General Offices. 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 home state, and local law enforcement. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.
You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).
For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.
For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226 for more information about preventing identity theft.
For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.
For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.
For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.
For Rhode Island residents: You may contact the Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, https://riag.ri.gov/.
Reporting of identity theft and obtaining a police report.
For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.
For Massachusetts residents: You have the right to obtain a police report.
For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.
For Rhode Island residents: You have the right to obtain a police report.

Placing a Security Freeze. You have a right to place a "security freeze" on your credit report, at no charge, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

You can place, temporarily lift, or permanently remove a security freeze on your credit report online, by phone, or by mail. You will need to provide certain personal information, such as address, date of birth, and Social Security number to request a security freeze and may be provided with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze. Information on how to place a security freeze with the credit reporting agencies is also contained in the links below:

https://www.equifax.com/personal/credit-report-services/
https://www.experian.com/freeze/center.html
https://www.transunion.com/credit-freeze

As of February 20, 2023, the reporting agencies allow you to place a credit freeze through the online, physical mail and phone numbers and request that you provide the information listed below. Where possible, please consult the websites listed above for the most up-to-date instructions.

Reporting Agency	Online	Physical Mail	Phone Number
Equifax	***Freeze request may be submitted via your minor's myEquifax account, which you can create here:*** https://my.equifax.com/consumer-registration/UCSC/#/personal-info	***Mail the Equifax Freeze Request Form to:*** Equifax Information Services LLC P.O. Box 105788 Atlanta, GA 30348-5788 ***Form may be found here:*** https://assets.equifax.com/assets/personal/Security_Freeze_Request_Form.pdf	888-298-0045
Experian	***Freeze request may be submitted here:*** https://www.experian.com/ncaconline/freeze	***Mail the request to:*** Experian Security Freeze, P.O. Box 9554, Allen, TX 75013 ***Request must include:*** • Full Name • Social security number • Complete address for last 2 years • Date of birth • One copy of a government issued identification card, such as a driver's license, state ID card, etc. • One copy of a utility bill, bank or insurance statement, etc.	888-397-3742

TransUnion	***Freeze request may be submitted via your TransUnion account, which you can create here:*** https://service.transunion.com/dss/orderStep1_form.page?	**Mail the request to:** TransUnion P.O. Box 160 Woodlyn, PA 19094 **Request must include:** • Full Name • Social security number • Complete address	888-909-8872

Fees associated with placing, temporarily lifting, or permanently removing a security freeze no longer apply at nationwide consumer reporting agencies.

Placing a Fraud Alert. To protect yourself from possible identity theft, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. You may obtain additional information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or security freeze on your credit report.

0000103030000

P

Also, please review any communications from Aetna, including Explanations of Benefits (EOBs), and call Member Services using the toll-free number on the back of your ID card if you see anything suspicious. We monitor for fraud and can work with you if you believe that your ID numbers are being used in an unauthorized manner.

More Information: Brightline is committed to data protection. We regularly review our physical and electronic safeguards to protect personal information, and we will continue to take appropriate steps to safeguard personal information and our systems. We deeply regret any inconvenience or concern this may have caused. Should you have any additional questions, you may contact us at [redacted] from 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays.

Sincerely,
Brightline