CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

December 22, 2023

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

To Whom It May Concern:

We serve as counsel for Meridian Behavioral Healthcare, Inc. ("Meridian")[1], located at 1565 SW Williston Road, Gainesville, FL 32608 and provide this notification to your Office of a recent data security incident suffered by Meridian. By providing this notice, Meridian does not waive any rights or defenses under New Hampshire law, including the data breach notification statute.

On August 11, 2023, Meridian discovered certain unauthorized activity within its computer systems. Upon discovery, Meridian immediately secured its network, reset passwords, and swiftly engaged a third-party team of forensic investigators to determine the full nature and scope of the incident. Following a thorough investigation, Meridian confirmed that a limited amount of information may have been accessed in connection with this incident.

On December 4, 2023, Meridian discovered that information related to fifteen (15) residents of New Hampshire was potentially impacted by this event. The information that could have been accessed may have included the individual's

. The potentially impacted information may include all or just one of the above listed types of information.

[1] Meridian is a Healthcare Covered Entity under the Health Insurance Portability and Accountability Act ("HIPAA"). See, 45 CFR 164.410.

Meridian provided written notice of this incident to the potentially impacted New Hampshire residents via First Class Mail on December 22, 2023. A copy of the notice letter is attached hereto as **Exhibit A**, which provides details of the incident, complimentary credit monitoring services for , and steps impacted individuals can take to protect their data. Meridian is taking proactive steps to ensure that all state and federal notification obligations are complied with due to this incident. This includes providing notice to the three major credit reporting agencies, the U.S. Department of Health and Human Services in accordance with the HIPAA Breach Notification Rule[2], and all applicable state regulators.

Please contact me should you have any questions.

Very truly yours,

Jordan Morgan, Esquire
CIPRIANI & WERNER, P.C.

[2] See, 45 CFR 164.400-414.

Exhibit A

MERIDIAN
Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

>>Mailing ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

<<Date>>

Re: <<Var Data - Header>>

Dear <<Name 1>>:

Meridian Behavioral Healthcare, Inc. ("Meridian") writes to notify you of a recent incident that may have impacted some of your personal health information described below.

We take the privacy and security of all information very seriously. While we have no evidence to suggest that any information was subject to actual or attempted misuse as a result of this incident, we are taking steps to proactively notify potentially impacted individuals out of an abundance of caution.

What Happened:

On August 11, 2023, Meridian discovered certain unauthorized activity within its computer systems. Upon discovery, Meridian immediately secured its network, reset passwords, and swiftly engaged a third-party team of forensic investigators to determine the full nature and scope of the incident. On December 4, 2023, following a thorough investigation, Meridian confirmed that a limited amount of information may have been accessed in connection with this incident.

At this time, there is no indication that any information has been misused. However, we are providing this notification to you out of an abundance of caution and so that you may take steps to safeguard your information if you feel it is necessary to do so.

What Information Was Involved:

The information that could have been accessed by the unauthorized individual(s) may have included your

. Importantly, the information potentially impacted varies for each individual, and in your case may include all, or just one of the above-listed types of information.

What Are We Doing:

Meridian has taken every step necessary to address the incident and is committed to fully protecting all of the information that you have entrusted to us. Upon learning of this incident, we immediately secured the network, reset passwords, and took steps to enhance the security of all information to help prevent similar incidents from occurring in the future.

Credit Monitoring:

As an additional safeguard for your information, Meridian has arranged for you to enroll, at no cost to you, in identity theft protection services through Identity Defense for <<CM Length>> of credit monitoring and fully managed identity theft recovery services. With this protection, Identity Defense will help you resolve issues if your identity is compromised. Please note the deadline to enroll is <<Enrollment Deadline>>. Due to state and federal privacy laws, Meridian cannot enroll you directly. If you wish to take advantage of this complimentary credit monitoring service, you must enroll yourself.

What You Can Do:

In addition to enrolling in the complimentary credit monitoring service detailed within, we recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on any of your accounts, please promptly change your password, take additional steps to protect your account, and notify your financial institution or company if applicable. Additionally, please report any suspicious incidents to local law enforcement and/or your State Attorney General. You can also review the enclosed "Steps You Can Take to Help Protect Your Information" for additional resources.

For More Information. Should you have additional questions or concerns regarding this matter, please do not hesitate to contact our dedicated call center at , Monday through Friday during the hours of 9:00 am and 9:00 pm Eastern Standard Time. You can also write us at 1565 SW Williston Road, Gainesville, FL 32608.

Sincerely,

Donald Savoie
President/Chief Executive Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a 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, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit 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 credit freeze 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. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim.

Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are <<RI #>> Rhode Island residents impacted by this incident.

Identity Defense

Enter your Activation Code: <<ActivationCode>>
Enrollment Deadline: <<Enrollment Deadline>>
Service Term: <<CM Length>>*

Identity Defense Complete

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- $1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Identity Defense, visit https://app.identitydefense.com/enrollment/activate/meri

1. Enter your unique Activation Code <<ActivationCode>>
2. Enter your Activation Code and click 'Redeem Code'.
3. Create Your Account
4. Enter your email address, create your password, and click 'Create Account'.
5. Register
6. Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
7. Complete Activation
8. Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at **1.866.622.9303.**