SUNSPIRE HEALTH

<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Re: Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

We write to inform you of a data privacy incident that may affect the security of your personal information. While we are unaware of any actual or attempted misuse of your information, we take this incident very seriously and are providing you with information and access to resources that you can use to better protect against the possibility of identity theft and fraud, if you feel it is appropriate to do so.

What Happened? On May 17, 2018, Sunspire Health ("Sunspire") learned that it was the target of a phishing email campaign that compromised several employee email account credentials. Sunspire immediately took steps to secure the email accounts and launched an in-depth investigation to determine whether any sensitive information was accessed or acquired.

Sunspire subsequently determined, with the help of third-party computer forensic investigators, that an unknown actor had gained access to certain Sunspire employee email accounts between March 1, 2018 and May 4, 2018. While the investigation into this incident is ongoing, on June 29, 2018, Sunspire determined that your information was contained in one of the compromised email accounts.

What Information Was Involved? While our investigation into this incident is ongoing, we have determined that information including your <<ClientDef1>><<ClientDef2>>(name, [data elements]) was contained in the compromised email accounts.

What is Sunspire doing? We take the security of information in our care very seriously. Since discovering this event, we have been working diligently with third-party forensic investigators to determine what happened and what information was accessible to the unknown actor, which is ongoing. This has involved a programmatic and manual data review process. Sunspire quickly initiated incident response and risk mitigation activities such as forcing password changes, conducting analysis of the network and applications to ensure there was no additional unauthorized access or any on-going threat to the Sunspire network. We also reviewed and made changes to existing security protocols. We are providing you with information about this event and about the steps you can take to better protect against misuse of your personal information, should you feel it appropriate to do so.

As an added precaution, we are also offering you access to one year of credit monitoring and identity theft restoration services through Kroll at no cost to you. The cost of this service will be paid for by Sunspire. We encourage you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Your Information." There you will find information on how to better protect against identity theft and fraud.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call 1-833-228-5709, Monday through Friday, 9 a.m. to 6 p.m. EST (excluding US holidays).

Sunspire takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Christopher Diamond
President & CEO of Sunspire
Sunspire Health

Kroll

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit 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.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Identity Monitoring

To help relieve concerns and restore confidence following this incident, Sunspire has secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.

*You have until **October 25, 2018** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-833-228-5709. Additional information describing your services is included with this letter.

Monitor Your Accounts

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits forms, and monitoring your free credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from $3 to $15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

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

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/
credit-freeze/place-credit-freeze

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

For Maryland residents, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us.

For North Carolina residents, the North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; by phone toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. Forty Rhode Island residents are potentially impacted by this incident. You have the right to file and obtain a police report if you ever experience identity theft or fraud. Please note that, in order to file a crime report or incident report with law enforcement for identity theft, you may be asked to provide some kind of proof that you have been a victim.

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 agencies 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 Oregon residents, the Oregon Attorney General can be reached at: Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096; 1-888-877-9392 Toll-Free Consumer Hotline; and www.doj.state.or.us.

Sunspire is located at: 160 Chubb Avenue, Suite 206, Lyndhurst, NJ 07071

SUNSPIRE HEALTH

SUNSPIRE HEALTH PROVIDES NOTICE OF DATA INCIDENT

Lyndhurst, New Jersey – July 16, 2018 – Sunspire Health ("Sunspire") is taking action after discovering that it became the target of a phishing email campaign that compromised several employee email account credentials.

Although there is no indication to date of actual or attempted misuse of patient information, Sunspire is notifying individuals whose records were or may have been subject to unauthorized access and providing these individuals with information and resources to help protect them against the possibility of identity theft or fraud. The company is also informing the U.S. Department of Health and Human Services and appropriate state authorities about this incident. Sunspire continues to investigate the incident and has implemented supplemental technical and administrative protections and training protocols to prevent similar occurrences in the future.

To better assist individuals who may have been affected by this event, Sunspire has established a toll-free privacy line and has dedicated personnel on hand to provide information on how to protect against the possibility of identity theft and fraud. All questions and concerns regarding how individuals may best protect themselves from potential harm resulting from this incident, including how to receive a free copy of one's credit report, and place a fraud alert or security freeze on one's credit file, may be directed to this line by calling 888-899-8301 between 8:30 a.m. and 5:30 p.m. EST (excluding US holidays) for a period of 90 days.

What Happened

Between April 10, 2018 and May 17, 2018, Sunspire learned that its employees became the target of a phishing email campaign that compromised several email accounts. Upon learning of this incident, Sunspire took immediate steps to secure the email accounts and has launched an investigation to determine whether any sensitive information was accessed. With the help of third-party computer forensic investigators, Sunspire has determined that unknown individuals may have gained access to certain Sunspire employee email accounts between March 1, 2018 and May 4, 2018. As part of this ongoing investigation, Sunspire recently determined that the compromised email accounts may have contained some patient information, which may include client names, dates of birth, Social Security numbers, treatment and diagnosis information, health insurance information. To date, there is no evidence the information in the emails has been misused in any way. Sunspire is providing notice to impacted individuals and will provide credit and identity monitoring services to such individuals at no charge.

About Sunspire Health

Sunspire is a network of addiction treatment facilities across the United States offering addiction recovery services, including detoxification, residential and outpatient treatment programs in settings designed to promote long-term healing. For more information, visit the company's web site at Sunspirehealth.com.

###

Media:
James Heins
ICR
203-682-8251

or

Darcie Robinson
ICR
203-682-8379