akerman

Thomas J. Kearney

Akerman LLP
The Victor Building
750 Ninth Street N.W., Suite 750
Washington, D.C. 20001
Tel: 202.393.6222
Fax: 954.393.5959

Dir: 202.824.1777
Dir Fax: 202.585.6231
thomas.kearney@akerman.com

June 11, 2020

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Via email: attorneygeneral@doj.nh.gov

Re: Data Security Incident

Dear Attorney General MacDonald:

We represent Sunrise Treatment Center, LLC ("Sunrise") with respect to a recent security incident. Pursuant to New Hampshire Revised Statutes Annotated § 359–C:20, we write to notify you that the personal information of one (1) New Hampshire resident may have been exposed, described in more detail below.

On February 27, 2020, Sunrise learned that the outside entity was able to use employee credentials to gain unauthorized access to the email account of one (1) Sunrise employee. Sunrise immediately began an investigation and determined on March 5, 2020, that the outside entity appeared to have gained unauthorized access on February 26, 2020 and February 27, 2020. On April 15, 2020, Sunrise's forensic investigator determined that personal information belonging to some Sunrise employees was contained within the affected email account and therefore was potentially accessed. The personal information stored in the affected email account include first and last name, home address, and social security number. The forensic investigation revealed that the primary purpose of the unauthorized access appears to be to cause Sunrise employees to wire money to a foreign bank account controlled by the outside entity. Because of procedures that Sunrise and its bank had in place, the theft attempt was discovered before any money could be wired to the foreign bank account. We have no evidence that the outside entity accessed or used any employee information in the affected email account.

Sunrise took steps to address this incident promptly after it was discovered, including

immediately terminating the unauthorized access to the employee email account and resetting all user account passwords. Sunrise also engaged a third-party specialist to perform an enterprise-wide security assessment and implemented additional technology safeguards to help prevent this type of incident from occurring again. As an added precaution, Sunrise is providing a credit monitoring service for 12 months at no cost to the affected New Hampshire resident.

Sunrise expects to notify the affected New Hampshire resident of this breach no later than June 12, 2020. If you have any questions or need additional information, please do not hesitate to contact me at thomas.kearney@akerman.com or (202) 824-1777.

Very truly yours,

Thomas J. Kearney

Enclosure

6460 Harrison Avenue, Suite 300
Cincinnati, OH 45247

June 12, 2020

F5984-L02-0000002 P001 T00001 **********MIXED AADC 159
SAMPLE A SAMPLE - L02 EMPLOYEE
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

RE: Important Security Notification
Please read this entire letter.

Dear Sample A Sample:

We are contacting you regarding a data security incident that has occurred on February 26 and 27, 2020 at Sunrise Treatment Center, LLC ("Sunrise"). This incident involved your first and last name and one or more of your date of birth, address, social security number, and in some cases driver's license number, financial account number, and health plan number. As a result, your personal information may have been potentially exposed to others. Please be assured that we have taken every step necessary to address the incident.

Over two days in February 2020 an outside entity accessed Sunrise data without authorization. On February 27, 2020, we learned that the outside entity was able to use employee credentials to gain unauthorized access to the email account of one (1) Sunrise employee. We immediately began an investigation and determined on March 5, 2020, that the outside entity appeared to have gained unauthorized access on February 26, 2020 and February 27, 2020. On April 15, 2020, our forensic investigator determined that personal information belonging to some of our employees was contained within the affected email accounts and therefore was potentially accessed. The potential access was limited to personal information contained in emails of the employee and did not include employee records.

Our forensic investigation revealed that the primary purpose of the unauthorized access appears to be to cause Sunrise employees to wire money to a foreign bank account controlled by the outside entity. Because of procedures that Sunrise and its bank had in place, the theft attempt was discovered before any money could be wired to the foreign bank account. We have no evidence that the outside entity accessed or used any personal information in the affected email accounts.

We take the privacy of personal information seriously and deeply regret that this incident happened. We took steps to address this incident promptly after it was discovered, including immediately terminating the unauthorized access to the employee email account and resetting all user account passwords. Upon learning of the incident, we investigated the incident. Additionally, we engaged a third-party specialist to perform an enterprise-wide security assessment and implemented additional technology safeguards to help prevent this type of incident from occurring again. While we have no evidence that the outside entity was trying to obtain the personal information of patients, we cannot be certain that your personally identifiable information was not accessed by an unauthorized person. Therefore, we are notifying you of the potential breach of your information and, in an abundance of caution, we are offering credit monitoring services.

What we are doing to protect your information:
To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **September 30, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: *https://www.experianidworks.com/credit*
- Provide your **activation code**: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 855-744-2743 by September 30, 2020**.** Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there. was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 855-744-2743. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at 855-744-2743.

Sincerely,

Dr. Jeffrey P. Bill, MD
Founder, CEO
Sunrise Treatment Center

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

The following information is for those individuals who want more information about the steps they can take to protect themselves.

Monitor Your Accounts

Monitor your credit and bank information for any suspicious or unauthorized activity. You may want to alert your bank or credit card company of this incident so they can monitor your accounts for suspicious activity. Notify your bank or credit card issuer if you notice any suspicious activity.

Get A Copy of Your Credit Report

You may obtain a copy of your credit report, free of charge, directly from each of the three credit reporting agencies once every twelve (12) months. To do so, please visit https://www.annualcreditreport.com or call toll-free 1-877-322-8228. Contact information for the three credit reporting agencies is included below.

Place a Fraud Alert

You may consider placing a fraud alert on your accounts. A fraud alert allows creditors to get a copy of your credit report as long as they take steps to verify your identity. For example, if you provide a telephone number, the business must call you to verify whether you are the person making the credit request. Fraud alerts may be effective at stopping someone from opening new credit accounts in your name, but they may not prevent the misuse of your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

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.

Place a Credit Freeze

Federal law allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. Below are instructions, with contact information, for placing and lifting a security freeze on your credit report. Please be aware, however, that a security freeze may delay, interfere with, or prevent the timely approval of any request you make for new loans, credit mortgages, employment, housing or other services.

SECURITY CREDIT FREEZE INSTRUCTIONS

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze.

To place a security freeze on your credit report, you must send a request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and Trans Union (www.transunion.com) at the addresses and telephone numbers below:

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

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

Transunion
TransUnion Security Freeze
Fraud Victim Assistance Department
P.O. Box 75013
Chester, PA 19022
1-888-909-8872
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, 1-877-IDTHEFT (438-4338), http://www.identitytheft.gov/

For residents of North Carolina: You may obtain information about preventing and avoiding identity theft from the North Carolina Attorney General:

> **Office of the Attorney General**, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1919-716-6000, https://ncdoj.gov/protecting-consumers/protecting-your-identity.