



October 31, 2023

Anjali C. Das
312.821.6164 (Direct)
anjali.das@wilsonelser.com

Karen I. Bridges
312.706.3023 (Direct)
karen.bridges@wilsonelser.com

Via Online Submission

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Notice of Data Security Incident

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker, LLP (“Wilson Elser”) represents Deer Oaks Behavioral Health (“Deer Oaks”), a mental healthcare provider based in San Antonio, Texas, with respect to a cybersecurity incident that was discovered by Deer Oaks on September 1, 2023 (hereinafter, the “Incident”). Please note Deer Oaks takes the security and privacy of the information within its control seriously, and has taken steps to prevent a similar incident from occurring in the future. This letter will serve as a notice of the Incident and to inform you of the steps Deer Oaks has taken in response to the Incident.

1. Nature of the Incident

On September 1, 2023, Deer Oaks became aware of potential unauthorized activity within its computer network. The unauthorized activity was immediately detected and isolated by Sophos antivirus software limiting the Incident to a one segment of Deer Oaks’ network. Upon discovery of the Incident, Deer Oaks engaged a specialized incident response vendor to secure its network and conduct a thorough forensic investigation to determine the nature and scope of the unauthorized activity.

Deer Oaks also conducted a review of the data maintained within the impacted server for purposes of providing notices to any patients whose information was contained therein. Deer Oaks completed its review on September 29, 2023. Based upon the results of its review, Deer Oaks determined that the following elements of personal information may have been accessed and/or acquired by an unauthorized individual: names, addresses, dates of birth, Social Security numbers,

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Indiana • Kentucky
Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Missouri • New Jersey • New Orleans • New York • Orlando • Philadelphia • Phoenix
San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

System.Object[]

diagnosis codes, insurance information, and treatment service type. The specific data elements that were impacted vary per individual. As of this writing, Deer Oaks has not received any reports of related identity theft, since the date of the Incident to the present.

2. Number of Maine residents affected.

Deer Oaks discovered that the Incident may have resulted in unauthorized exposure of information pertaining to four hundred and sixty (460) Maine residents. Notification letters to the individuals were mailed on October 31, 2023, by First Class Mail. A sample copy of the notification letter is attached hereto as **Exhibit A**.

3. Steps taken in response to the Incident.

Deer Oaks is committed to ensuring the security and privacy of all personal information within its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, engaged a specialized cybersecurity firm to conduct a forensic investigation in order to determine the nature and scope of the Incident. Additionally, Deer Oaks has taken steps to strengthen its security posture to prevent a similar event from occurring again in the future.

Deer Oaks is also offering twelve (12) months of complimentary credit monitoring and identity theft restoration services through IDX to potentially affected individuals residing in Maine to help protect their identity. Additionally, Deer Oaks provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies and Federal Trade Commission, information on how to obtain a free credit report, and a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports.

4. Contact Information

Deer Oaks remains dedicated to protecting the sensitive information within its control. Should you have any questions or need additional information, please do not hesitate to contact me at karen.bridges@wilsonelser.com or 312.706.3023.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Karen I. Bridges

Karen I. Bridges

EXHIBIT A





<<Return Address>>
<<City>>, <<State>> <<Zip>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:
<https://response.idx.us/Deer-Oak>

Notice of Data Incident

Dear <<First Name>> <<Last Name>>,

Deer Oaks Behavioral Health (“Deer Oaks”) is writing to inform you of a recent cybersecurity incident that may have involved your protected health information (“PHI”). Deer Oaks takes the privacy of patient information very seriously and sincerely apologizes for any inconvenience this Incident may cause. This letter contains details about the Incident, steps we have taken in response to mitigate any risk, and services we are making available to protect your information.

What Happened

On September 1, 2023, Deer Oaks discovered that a segment of its computer systems had been subjected to unauthorized access and ransomware (the “Incident”). The unauthorized activity was immediately detected and isolated by Sophos antivirus software limiting the Incident to a one segment of Deer Oaks’ network.

Upon discovery of the Incident, Deer Oaks engaged a specialized cyber forensics team to investigate the root cause and confirm the extent of the unauthorized activity. The forensic investigation confirmed unauthorized access to Deer Oaks computer systems first occurring on _____.

Upon confirming the unauthorized access, Deer Oaks conducted a review of the data maintained within the impacted server for purposes of providing notices to any patients whose information was contained therein. Deer Oaks completed its review on September 29, 2023. Based upon the results of its review, Deer Oaks is notifying all those patients whose information may have been accessed by an unauthorized user as a result of the Incident.

What Information Was Involved

The investigation confirmed that patient information maintained within the compromised computer systems may have been subject to unauthorized access. The data contained in this system may include protected health information such as your: name, address, [Data Elements].

We note Deer Oaks has not received any reports of fraudulent activity to date that resulted from this Incident.

What We Are Doing

Deer Oaks takes the privacy and security of our personal information very seriously, and has taken steps to prevent a similar event from occurring in the future.

In addition, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: [12 months/24 months] of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling [TFN], going to <https://response.idx.us/Deer-Oak>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is [Enrollment Deadline].

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call [TFN] or go to <https://response.idx.us/Deer-Oak> for assistance or for any additional questions you may have.

Sincerely,

Deer Oaks Behavioral Health



Recommended Steps to help Protect your Information

1. Website and Enrollment. Scan the QR image or go to <https://response.idx.us/Deer-Oak> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at [TFN] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

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

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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

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 a 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. You can 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.

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/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

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

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.