PARK PLACE
BEHAVIORAL HEALTH CARE

Return to IDX:
P.O. Box 1907
Suwanee, GA 30024

Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: December 23, 2026

To Enroll, Scan the QR Code Below:

[redacted]

SCAN ME

Or Visit:
[redacted]

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

VIA FIRST-CLASS MAIL

September 23, 2026

Re: Notice of Data Incident/Breach

Dear <FirstName> <LastName>,

Osceola Mental Health ("Osceola") values and respects the privacy of your personal information, which is why we are notifying you of a recent incident that may have involved some of your personal information. Below you will find information about what happened, steps we are taking, and resources and additional guidance to help you protect your information.

What Happened?

On July 23, 2026, Osceola became aware of unusual activity on its computer systems. Upon discovery of this incident, Osceola immediately secured the environment and promptly engaged a specialized third-party cybersecurity firm to conduct a comprehensive investigation to determine the nature and scope of the incident. The forensics investigation was completed on August 19, 2026.

Osceola has determined that certain information stored on our systems was copied by an unauthorized party. Thereafter, Osceola conducted a thorough review of the impacted files. Osceola is notifying all individuals whose personal information may have been exposed as a result of this incident via U.S. mail to the extent we have their mailing addresses. On September 17, 2026, Osceola finalized the list of individuals to notify. As of this writing, Osceola has not received any reports of misused personal information or identity theft since the date of the incident.

What Information Was Involved?

We conducted an extensive and comprehensive review to identify the specific individuals and the type of data that was impacted. The type of personal information that may have been exposed varied for each person as specified in the individual notice letters. The information may have included one or more of the following data elements: Social Security number, driver's license number or other government-issued ID number, financial account information, health information, and/or health insurance information.

What We Are Doing

Data privacy and security are among our highest priorities, and we are committed to doing everything we can to protect the privacy and security of personal information within our care. Since the discovery of the incident, we moved quickly to investigate, respond, and confirm the security of our computer systems. Specifically, we reset all user account credentials, installed endpoint detection and response software to monitor our network system, refined the security of our remote access methods, restored operations in a safe and secure mode, and will continue to take steps to mitigate the risk of future harm. Finally, we are providing affected individuals with complimentary credit monitoring and identity theft restoration services.

We are offering identity theft protection services through IDX, 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 identity 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 take advantage of the complimentary credit monitoring and identify theft protection we are making available to you. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

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: <<Unique Code>>.

In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. Enrollment requires an internet connection and e-mail account and may not be available to minors under the age of eighteen (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.

Additionally, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. You can find more information on steps to protect yourself against identity theft identity theft in the enclosed *Additional Resources to Help Protect Your Information* sheet.

Contact Information

We value the trust you place in us and sincerely regret any concern or inconvenience this matter may cause. Rest assured we remain dedicated to ensuring the privacy and security of all information in our control. Should you have any questions or concerns about this incident or need assistance enrolling in credit monitoring, please call [redacted] during the hours of 9:00 a.m. to 9:00 p.m. Eastern Time, Monday through Friday (excluding U.S. national holidays).

Sincerely,

Osceola Mental Health d/b/a Park Place Behavioral Healthcare

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity. You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies. You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 www.equifax.com/personal/credit-report-services
TransUnion	P.O. Box 1000 Chester, PA 19016 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

For Iowa and Oregon residents, you are advised to report suspected incidents of identity theft to local law enforcement, to your respective Attorney General, and the FTC.

For Massachusetts residents, you are advised of your right to obtain a police report in connection with this incident.

For District of Columbia residents, the Attorney General may be contacted at the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

For Maryland residents, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at www.oag.state.md.us/Consumer, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491. Osceola Mental Health d/b/a Park Place Behavioral Healthcare is located at 200 Park Place Blvd, Kissimmee, FL 34741 and can be reached at 407-846-0023.

For New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also 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 violators. 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 at 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, you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, www.ag.ny.gov.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at www.ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/.

For Rhode Island residents, you may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.