

Data Breach Notification Center
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[REDACTED]

December 23, 2024

Dear [REDACTED]

American Addiction Centers, Inc., and its affiliated providers, including AdCare, the Greenhouse, Desert Hope Center, Oxford Treatment Center, Recovery First, Sunrise House, River Oaks Treatment Center, and Laguna Treatment Hospital, (“AAC” or “we”) believe that the privacy and security of your health information is important and are committed to protecting it. We are writing to notify you that a cybersecurity incident at AAC may have involved some of your personal information. This notice explains the incident, the measures we have taken in response and the steps individuals can take for further protection.

What Happened: On or around September 26, 2024, AAC learned that it was experiencing a cybersecurity incident. AAC immediately launched an investigation and engaged leading third-party cybersecurity experts to assist. AAC also notified law enforcement and swiftly contained the incident. On October 3, 2024, the investigation determined that an unauthorized party had taken some data from AAC’s systems between September 23 and September 26, 2024. A thorough review of the impacted data was conducted to identify what information was involved and the individuals to whom the data related. At this time, we are not aware of any identity theft or fraud related to the use of any affected individual’s information, including yours.

What Information Was Involved: The impacted data may have included the following information about you: name, address, phone number, date of birth, medical record number or other identifier, social security number, and health insurance information. The affected data did not include your treatment information, or payment card data.

What We Are Doing: After becoming aware of the incident, AAC immediately took additional protective measures to safeguard its systems and worked with leading cybersecurity experts to conduct a comprehensive investigation of the incident. AAC notified law enforcement and is cooperating with their investigation. To help prevent similar incidents from happening in the future, AAC implemented and is continuing to implement additional security protocols designed to enhance the security of its IT system environments.

We want you to feel confident that your data is secure. To help protect your identity, we are offering you Single Bureau Credit Monitoring, Single Bureau Credit Report, and Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. Alerts will be sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Cyberscout credit monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED].

In order for you to receive the monitoring services described above, you must enroll by March 31, 2025. The enrollment requires an internet connection and email account and may not be available to minors under the age of 18. 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.

What You Can Do: Although we have no evidence that any of your information has been subject to identity theft or fraud, you should always remain alert by regularly reviewing your account statements and monitoring free credit reports, and immediately reporting to your banks and other financial institutions any suspicious activity involving your accounts. The enclosed “General Information about Identity Theft Protection” page provides further information about ways to do this. We also encourage you to enroll in the identity monitoring services that we have offered to you.

For More Information: If you have questions, please call our dedicated, toll-free call center at 1-833-833-2770 and supply the specialist with your unique code listed above. The hotline operating hours are Monday through Friday between 8:00 a.m. and 8:00 p.m. Eastern Time, excluding major U.S. holidays.

We regret that this incident occurred and any concern it may cause. We take the confidentiality and security of personal information very seriously and will continue to take steps to prevent a similar incident from occurring in the future.

Sincerely,

American Addiction Centers, Inc.

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling 1-877-322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. **You may contact the nationwide credit reporting agencies at:**

Equifax	Experian	TransUnion
P.O. Box 105788 Atlanta, GA 30348 www.equifax.com 1-800-525-6285	P.O. Box 9554 Allen, TX 75013 www.experian.com 1-888-397-3742	P.O. Box 2000 Chester, PA 19016 www.transunion.com 1-800-680-7289

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Place a Security Freeze on your Credit Report. You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. You can place a freeze and lift a security freeze on your credit report free of charge.

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

If you are a District of Columbia resident, you may contact and obtain information from your attorney general at: 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.

If you are an Iowa resident, state law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590.

If you are a Maryland resident, you can contact the Maryland Office of the Attorney General, Consumer Protection Division at: 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023.

If you are a Massachusetts resident, under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/contact-the-attorney-generals-office.

If you are a New Mexico resident, you have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act or www.ftc.gov.

If you are a New York resident, you can contact the New York Office of the Attorney General at www.ag.ny.gov, 1-800-771-7755; the New York Department of State, www.dos.ny.gov, 1-800-697-1220; and the New York Division of State Police, www.ny.gov/agencies/division-state-police, (914) 834-9111.

If you are a North Carolina resident, you can contact the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, <https://ncdoj.gov>, 1-877-566-7226.

If you are an Oregon resident, state law advises you to report any suspected identity theft to law enforcement or to the FTC.

If you are a Rhode Island resident, you have the right to obtain a police report. You also have the right to request a security freeze, as described above. You can also contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, (401) 274-4400 or file a police report by contacting (401) 444-1000.

If you are a West Virginia resident, you have the right to ask that nationwide consumer reporting agencies place “fraud alerts” in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

Data Breach Notification Center
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

December 23, 2024

Notice of Data Breach

Dear [REDACTED]:

American Addiction Centers, Inc. (“AAC”) believes that the privacy and security of your personal information is important and is committed to protecting it. We are writing to notify you of a recent incident at AAC that may have involved some of your personal information that we maintained in our role as your employer. This notice explains the incident, the measures we have taken in response and the steps individuals can take for further protection.

WHAT HAPPENED

On or around September 26, 2024, AAC learned that it was experiencing a cybersecurity incident. AAC immediately launched an investigation and engaged leading third-party cybersecurity experts to assist. AAC also notified law enforcement and swiftly contained the incident. On October 3, 2024, the investigation determined that an unauthorized party had taken some data from AAC’s systems between September 23 and September 26, 2024. A thorough review of the impacted data was conducted to identify what information was involved and the individuals to whom the data related. At this time, we are not aware of any identity theft or fraud related to the use of any affected individual’s information, including yours.

WHAT INFORMATION WAS INVOLVED

The impacted data may have included your personal information related to your current and/or former employment with AAC and its predecessor companies, such as your name, date of birth, social security number, government identifiers such as driver’s license or passport number, benefits information, such as health insurance information and retirement account information, and medical information you may have provided in connection with leave requests or for other purposes.

WHAT WE ARE DOING

After becoming aware of the incident, AAC immediately took additional protective measures to safeguard its systems and worked with leading cybersecurity experts to conduct a comprehensive investigation of the incident. AAC notified law enforcement and is cooperating with their investigation. To help prevent similar incidents from happening in the future, AAC implemented and is continuing to implement additional security protocols designed to enhance the security of its IT system environments.

We want you to feel confident that your data is secure. To help protect your identity, we are offering you Single Bureau Credit Monitoring, Single Bureau Credit Report, and Single Bureau Credit Score services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. Alerts will be sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

[REDACTED]

To enroll in Cyberscout credit monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED].

In order for you to receive the monitoring services described above, you must enroll by March 31, 2025. The enrollment requires an internet connection and email account and may not be available to minors under the age of 18. 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.

WHAT YOU CAN DO

Although we have no evidence that any of your information has been subject to identity theft or fraud, you should always remain alert by regularly reviewing your account statements and monitoring free credit reports, and immediately reporting to your banks and other financial institutions any suspicious activity involving your accounts. The enclosed "General Information about Identity Theft Protection" page provides further information about ways to do this. We also encourage you to enroll in the identity monitoring services that we have offered to you.

FOR MORE INFORMATION

If you have questions, please call our dedicated, toll-free call center at [REDACTED] and supply the specialist with your unique code listed above. The hotline operating hours are Monday through Friday between 8:00 a.m. and 8:00 p.m. Eastern Time, excluding major U.S. holidays.

We regret that this incident occurred and any concern it may cause. We take the confidentiality and security of personal information very seriously and will continue to take steps to prevent a similar incident from occurring in the future.

Sincerely,

American Addiction Centers, Inc.

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling 1-877-322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. **You may contact the nationwide credit reporting agencies at:**

Equifax	Experian	TransUnion
P.O. Box 105788 Atlanta, GA 30348 www.equifax.com 1-800-525-6285	P.O. Box 9554 Allen, TX 75013 www.experian.com 1-888-397-3742	P.O. Box 2000 Chester, PA 19016 www.transunion.com 1-800-680-7289

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Place a Security Freeze on your Credit Report. You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. You can place a freeze and lift a security freeze on your credit report free of charge.

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

If you are a District of Columbia resident, you may contact and obtain information from your attorney general at: 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.

If you are an Iowa resident, state law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590.

If you are a Maryland resident, you can contact the Maryland Office of the Attorney General, Consumer Protection Division at: 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023.

If you are a Massachusetts resident, under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/contact-the-attorney-generals-office.

If you are a New Mexico resident, you have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act or www.ftc.gov.

If you are a New York resident, you can contact the New York Office of the Attorney General at www.ag.ny.gov, 1-800-771-7755; the New York Department of State, www.dos.ny.gov, 1-800-697-1220; and the New York Division of State Police, www.ny.gov/agencies/division-state-police, (914) 834-9111.

If you are a North Carolina resident, you can contact the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, <https://ncdoj.gov>, 1-877-566-7226.

If you are an Oregon resident, state law advises you to report any suspected identity theft to law enforcement or to the FTC.

If you are a Rhode Island resident, you have the right to obtain a police report. You also have the right to request a security freeze, as described above. You can also contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, (401) 274-4400 or file a police report by contacting (401) 444-1000.

If you are a West Virginia resident, you have the right to ask that nationwide consumer reporting agencies place “fraud alerts” in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.