

APPENDIX

On June 5, 2026, American Addiction Centers (“AAC”) learned of suspicious activity in its Salesforce environment. AAC immediately implemented its incident response protocols, took measures to contain the activity, and initiated an investigation. On June 8, 2026, AAC determined that an unauthorized third-party acquired certain information from AAC’s Salesforce instance on May 12, 2026. Importantly, this incident did not involve any access to AAC’s internal systems, network, or health records application.

The information involved contained the name, contact information, and a brief description an individual provided regarding their health for approximately 1,155 Washington residents. For a small number of these individuals, their Social Security number (one Washington resident) and/or health insurance information (seven Washington residents) was also involved.

On August 7, 2026, AAC began mailing notification letters to affected individuals via USPS First-Class mail in accordance with the Health Insurance Portability & Accountability Act (45 CFR 164.404) and/or Wash. Rev. Code § 19.255.010. A copy of the notification letter is enclosed. AAC is offering eligible individuals a complimentary offer of credit monitoring and identity theft protection services. Additionally, AAC has established a dedicated, toll-free call center to answer any questions individuals may have about the incident.

To help prevent a similar incident from occurring in the future, AAC has implemented, and will continue to adopt, additional safeguards to protect and monitor its Salesforce environment.



Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

<<CA Only Text>>

Dear <<Full Name>>:

American Addiction Centers (“AAC”) takes the privacy and security of the information in our possession very seriously. We are writing to notify you of a security incident that occurred through a third-party vendor and may have involved some of your information.

What Happened? On June 5, 2026, we learned of suspicious activity in our Salesforce environment. We immediately implemented our incident response protocols, took measures to contain the activity, and initiated an investigation. On June 8, 2026, we determined that an unauthorized third-party acquired certain information from our Salesforce instance on May 12, 2026. Importantly, this incident did not involve any access to our systems, network, or health records application.

What Information Was Involved? The information involved contained your name, contact information, Social Security number, and a brief description you provided of your health. This information was not pulled from our electronic health records application, and was instead limited to information obtained during an initial outreach to AAC.

What We Are Doing. We wanted to notify you of this incident and assure you we take this matter very seriously. To help prevent a similar incident from occurring in the future, we have implemented, and will continue to adopt, additional safeguards to protect and monitor our Salesforce environment.

What You Can Do. While we do not have evidence that your information was or will be misused, we recommend that you regularly review statements that you receive from your health insurer or healthcare providers. If you see charges for services that you did not receive, please contact the insurer or provider immediately. Additionally, out of an abundance of caution, to help protect your identity, we are offering you a complimentary <<CM Duration>> month membership of Privacy Solutions ID through Epiq. For more information on identity theft prevention and Privacy Solutions ID, including instructions on how to activate the complimentary <<CM Duration>> month membership, please see the additional information provided in this letter.

For More Information. We deeply regret any concern or inconvenience this incident may have caused you. If you have any questions, please call 1-888-650-3763, available Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

American Addiction Centers



Activation Code: <<ACTIVATION CODE>>
Enrollment Deadline: <<ENROLLMENT DEADLINE>>
Coverage Length: <<CM Duration>> Months

Epiq - Privacy Solutions ID
1B Credit Monitoring – Basic

How To Enroll:

- 1) Visit www.privacysolutionsid.com and click “Activate Account”
- 2) Enter the following activation code, <<Activation Code>> and complete the enrollment form
- 3) Complete the identity verification process
- 4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
- 5) Enter your log-in credentials
- 6) You will be directed to your dashboard and activation is complete!

Product Features:

1-Bureau Credit Monitoring with Alerts

Monitors your credit file(s) for key changes, with alerts such as credit inquiries, new accounts, and public records.

Dark Web Monitoring (Basic)

Monitors one email address, phone, name, DOB, and SSN on the dark web. Includes retrospective report as well as ongoing monitoring.

Credit Protection

3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Change of Address Monitoring

Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users' current or past addresses.

Identity Restoration & Lost Wallet Assistance

Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 1B Credit Monitoring - Basic, please call directly at **866.675.2006**, Monday-Friday 9:00 a.m. to 5:30 p.m., ET.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-833-799-5355

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

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.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov. AAC can be reached at 500 Wilson Pike Circle, Suite 360 Brentwood, TN 37027; Tel: (888) 987-1784.

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.marylandattorneygeneral.gov/.

Massachusetts: Under Massachusetts law, you have the right to file and obtain a copy of a police report. 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/ago/contact-us.html

New York: 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, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves <<RI Count>> individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. 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: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

New Mexico Residents: A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.