

May 23, 2023

Via Email

Attorney General Brian E. Frosh
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Frosh:

Constangy Brooks Smith & Prophete LLP represents American Addiction Centers: ("AAC") in connection with a recent data security incident described in greater detail below.

1. Nature of the security Incident.

On April 24, 2023, AAC discovered that during the month of April 2023, one of its employees, while in the process of performing the employee's job functions, inappropriately accessed and stole some patients' credit card numbers and used those credit card numbers to make unauthorized purchases. In response, ACC began an internal investigation, and upon confirming what the employee had done, the employee was terminated, and the incident was reported to law enforcement. As part of their investigation, ACC took steps to identify all patients whose personal information may have been at risk of being accessed by this person. On May 9, 2023, ACC completed their investigation, which determined that the employee had access to some patient names, payment card numbers, expiration dates, and security codes, which is the reason for this notification. Since that time, ACC has been diligently collecting up-to-date address information needed to notify all potentially affected individuals.

2. Number of Maryland residents affected.

ACC notified one Maryland residents of this incident via first class U.S. mail on May 19, 2023. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as ACC learned of this incident, ACC took the steps described above to investigate. When the investigation confirmed the employee's conduct, the employee was terminated, and the incident was reported to law enforcement. ACC will cooperate with any resulting investigation.

As a result of this incident, out of an abundance of caution, ACC has notified patients about this event, provided them with information about steps that can taken to help protect their information and offered them a complimentary identity protection services through IDX. These services include 12 months of credit and dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services.

4. Contact information.

ACC remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me.

Best regards,

A handwritten signature in black ink, appearing to read "LB Nickle".

Lindsay B. Nickle
Partner

Enclosure: Sample Notification Letter

[REDACTED]
[REDACTED]
[REDACTED]

May 19, 2023

Subject: Notice of Data Security Incident

Dear [REDACTED]:

American Addiction Centers (“AAC”) is writing to inform you about a recent data security incident that may have involved your personal information. AAC takes the privacy and security of all information within its possession very seriously. We are writing to notify you about the incident, provide you with information about steps you can take to help protect your personal information, and offer you the opportunity to enroll in complimentary identity protection services that AAC is making available to you.

What Happened? On April 24, 2023, AAC learned that during the month of April 2023, one of its employees inappropriately accessed some patient belongings, stole some patients’ credit card numbers, and used those credit card numbers to make unauthorized purchases. As soon as we learned about the situation, we began an internal investigation, and upon confirming what the employee had done, the employee was terminated, and the incident was reported to law enforcement. As part of our investigation, we took steps to identify all patients whose personal information may have been at risk of being accessed by this person. On May 9, 2023, we completed our investigation, which determined that the employee may have had an opportunity to access your information, and we are notifying you so that you can take steps to protect your information.

What Information Was Involved? The information involved may have included your name, payment card number, expiration date, and security code.

What Are We Doing? As soon as we discovered this incident, we took the steps described above, and we plan to fully cooperate with any law enforcement investigation. We also are notifying you about this event, providing you with information about steps you can take to help protect your information and offering you complimentary identity protection services through IDX – a data breach and recovery services expert. These services include 12 months of credit¹ and dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. Please note that the deadline to enroll in these services is August 19, 2023.

¹ To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

To Enroll, Please Call:
1-800-939-4170

Or Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code: [REDACTED]

What Can You Do? ACC recommends that you review the guidance included with this letter about how to protect your information. You can also enroll in the complimentary identity protection services being offered to you by using the Enrollment Code provided above.

For More Information: Further information about how to help protect your information appears on the following page. If you have questions about this matter, please reach out to Kimberly Speakman via email at kspeakman@ContactAAC.com or telephone at 615-732-1577. If you need assistance enrolling in the complimentary services being offered to you, please call IDX at 1-800-939-4170 from 8:00 A.M. to 8:00 P.M. Central Time, Monday through Friday (excluding holidays).

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'Kimberly D. Speakman', is positioned above the typed name and title.

Kimberly D. Speakman, MA, LPC/MHSP, CHC
Chief Compliance Officer
Oxford Treatment Center
American Addiction Centers
297 County Road 244
Etta, MS 38627

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-800-831-5614
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

Maryland Attorney General

St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Rev. December, 2022