

NOTICE OF BLACKBAUD DATA EVENT
SEPTEMBER 14, 2020

On Thursday, July 16, 2020, Prelude Behavioral Services, formerly MECCA, (“Prelude”) received notification from one of its third-party vendors, Blackbaud, Inc. (“Blackbaud”), of a cyber incident. Blackbaud is a cloud computing provider that offers financial accounting tools to non-profit organizations, including Prelude. Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic consultants to investigate. Following its investigation, Blackbaud notified its customers, including Prelude, that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020.

Upon learning of the Blackbaud incident, Prelude immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Prelude data, and to determine what, if any, sensitive Prelude data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. On September 3, 2020, Prelude’s investigation determined that the information potentially affected may have contained personal information.

What Information Was Involved? Our investigation determined that the involved Blackbaud systems potentially identified certain individuals as current or former Prelude patients, by virtue of refunds issued for health-related services provided by Prelude. The impacted information included only the affected patients’ names and addresses. **The impacted information did not contain our patients’ Social Security Number, financial account information, payment card information, driver’s license number or other medical/health insurance information.** Please note that, to date, we have not received any information from Blackbaud that Prelude’s information was specifically accessed or acquired by the cyber criminal, but this possibility could not be ruled out.

What is Prelude Doing? The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. As part of our ongoing commitment to the security of information in our care, we are working to review our existing policies and procedures regarding our third-party vendors, and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. We will also be notifying certain state and federal regulators, as required. Additionally, while we are unaware of any actual or attempted misuse of our patient information, in an abundance of caution, we are notifying potentially impacted individuals so that they may take further steps to protect their information, should they feel it appropriate to do so.

What Can Impacted Individuals Do? Potentially affected individuals seeking additional information regarding this incident, may contact Prelude at info@preludeiowa.org. They may also write to Prelude Behavioral Services at: 430 Southgate Ave Iowa City, IA 52240. Finally, potentially affected individuals may also consider the information and resources outlined below.

Monitor Your Accounts

Prelude encourages you to remain vigilant against incidents of identity theft and fraud, promptly change any involved account passwords, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three (3) major credit bureaus directly to request a free copy of your credit report.

You have the 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. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you lived over the prior five (5) years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a one (1) year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 2002
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); or 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 have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.