Jennifer S. Stegmaier
312.821.6167 (direct)
Jennifer.Stegmaier@wilsonelser.com

May 9, 2024

Via Online Submission

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Notice Re: Data Security Incident Involving Bridgeway Center, Inc.

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Bridgeway Center, Inc. ("Bridgeway"), a mental health service provider located at 205 Shell Avenue, Building A, Fort Walton Beach, FL 32548, with respect to a recent data security incident first discovered by Bridgeway on February 22, 2024 (hereinafter, the "Incident"). Please note Bridgeway takes the security and privacy of the information within its control very seriously and has taken steps to prevent a similar incident from occurring in the future. This letter will serve to provide you with information regarding the nature of the Incident, what data may have been compromised, and the steps that Bridgeway has taken in response to the Incident.

1. Nature of the Incident.

On February 22, 2024, Bridgeway discovered unauthorized activity within its network that may have resulted in unauthorized access to sensitive information of its clients and employees. Upon discovery of the Incident, Bridgeway promptly engaged a specialized cybersecurity incident response vendor to secure its network and conduct a forensic investigation to determine the source and scope of the unauthorized activity. The forensic investigation, which concluded on March 18, 2024, determined the unauthorized activity occurred from February 21, 2024, until February 23, 2024. While evidence from the forensic investigation indicated there was no mass exfiltration of data from Bridgeway's environment, the findings could not confirm that sensitive personal information within Bridgeway's computer systems was not accessed by an unauthorized user.

Based on these findings, Bridgeway conducted a review of the impacted computer systems to identify the specific individuals and the types of information that may have been compromised.

While the investigation was ongoing, on March 22, 2024, Bridgeway posted a notice of the Incident on the homepage of its website and published a notice of the Incident with The Northwest Florida Daily News a newspaper printed and published in Okaloosa County where Bridgeway's clients reside. Bridgeway completed its review of the impacted data on April 22, 2024.

Upon completing its review, Bridgeway engaged a thirty-party mailing vendor to assist with mailing notice letters to the affected individuals, provide a ninety (90) day call center for individuals to contact should they have additional questions regarding the Incident, and offer affected individuals complimentary credit monitoring and identity theft protection services.

2. What Information Was Involved?

Bridgeway has determined that the following types of personally identifiable information may have been impacted: Social Security number, driver license number, military identification number, date of birth, therapist/doctor notes, mental or physical condition/treatment, diagnosis information, medical procedure information, date of service, medical record number, sickness certificate, and prescription information. The information impacted varies by individual.

Please note that to date there has been no evidence to indicate that any individuals' personal information has been misused as a result of the Incident.

3. Number of Maine Residents Affected.

Based on the results of the forensic investigation and data review, Bridgeway determined that information pertaining to eight (8) Maine residents was impacted as a result of the Incident. Notification letters to the affected individuals were sent by U.S. First Class Mail on May 8, 2024. A sample copy of the notification is attached hereto as **Exhibit A**.

4. Steps taken in Response to the Incident.

Bridgeway is committed to ensuring the security and privacy of all personal information within its control and has taken steps to prevent a similar incident from occurring in the future. Since the discovery of the Incident, Bridgeway moved quickly to investigate, respond, and confirm the security of its systems by immediately shutting down its network, implementing necessary patches, and engaging a specialized incident response vendor to secure its network and conduct a forensic investigation.

In addition, Bridgeway implemented security enhancement measures to prevent a similar incident from occurring in the future, such as strengthening password requirements, implementing new technical and physical safeguards to secure the data within its possession, and providing additional cybersecurity training for its employees.

Bridgeway is also offering twelve (12) months of complimentary credit monitoring and identity theft restoration services to the impacted individuals residing in the State of Maine to help protect their identity. In addition, Bridgeway provided guidance to affected individuals on how to: better protect against identity theft and fraud, place a fraud alert and security freeze on one's credit file,

contact the national consumer reporting agencies, obtain a free credit report, remain vigilant for incidents of fraud and identity theft, and contact the Federal Trade Commission.

5. Contact Information.

Bridgeway remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Jennifer.stegmaier@wilsonelser.com or 312-821-6167.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Jennifer S. Stegmaier

EXHIBIT A

Bridgeway Center, Inc
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

May 8, 2024

Via First-Class Mail

0000101102G0500

P

Notice of Security Incident

Dear [redacted],

Bridgeway Center, Inc. ("Bridgeway Center") is writing to inform you of a recent data security incident that may have resulted in unauthorized access to your sensitive personal information. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened?

On February 21, 2024, Bridgeway Center detected unusual activity on its network. Upon discovery of this incident, Bridgeway Center immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm to assist with securing the environment, as well as to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensic investigation found evidence of unauthorized access to Bridgeway Center's computer systems.

Based on these findings, Bridgeway Center conducted a review of the affected systems to identify the specific individuals and the types of information that may have been compromised. On April 22, 2024, Bridgeway Center finalized the list of individuals to notify.

What Information Was Involved?

Although Bridgeway Center has no evidence that any sensitive information has been misused by third parties as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency. Based on the investigation, the following information related to you may have been subject to unauthorized access: [redacted].

What We Are Doing

Data privacy and security is among Bridgeway Center's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Since the discovery of the incident, Bridgeway Center moved quickly to investigate, respond, and confirm the security of our systems. Specifically, Bridgeway Center disconnected all access to its network, changed administrative credentials, restored operations in a safe and secure mode, enhanced its network security measures, and took steps and will continue to take steps to mitigate the risk of future harm.

In response to the incident, Bridgeway Center is providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, Bridgeway Center is providing you with proactive fraud assistance to help with any questions that you might have or in 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.

What You Can Do

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. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

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: [redacted]. In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. Enrolment 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.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call [redacted] (toll free) Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

Bridgeway Center sincerely regrets any concern or inconvenience this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Bridgeway Center, Inc.

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Identity Protection PIN: You can get a six-digit Identity Protection PIN to prevent someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. An IP PIN is used by the IRS to verify your identity when filing your electronic or paper tax return. To receive an IP Pin, you must register to validate your identity at IRS.gov. Use the Get an IP PIN tool available between mid-January through mid-November to receive your IP PIN.

https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin

Security Freeze: You have the right to place a security freeze on your credit report. 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 need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

File Police Report: You have the right to file or obtain a police report if you experience identity fraud.

Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: 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), 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. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You 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 residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of *Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island:* You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General - Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street**,** Chicago, IL 60601**;** 1-866-999-5630**;** www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division**:** 200 St. Paul Place**,** 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General - Consumer Protection Division**:** 9001 Mail Service Center, Raleigh, NC 27699**;** 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903**;** 1-401-274-4400**;** www.riag.ri.gov