WHITEFORD, TAYLOR & PRESTON L.L.P.

SPENCER S. POLLOCK
DIRECT LINE (410) 832-2002
DIRECT FAX (410) 339-4028
SPollock@wtplaw.com

TOWSON COMMONS, SUITE 300
ONE WEST PENNSYLVANIA AVENUE
TOWSON, MARYLAND 21204-5025
MAIN TELEPHONE (410) 832-2000
FACSIMILE (410) 832-2015

DELAWARE*
DISTRICT OF COLUMBIA
KENTUCKY
MARYLAND
NEW YORK
PENNSYLVANIA
VIRGINIA

WWW.WTPLAW.COM
(800) 987-8705

September 15, 2021

Privileged and Confidential
(SUBMITTED ONLY VIA THE ONLINE PORTAL AT https://appengine.egov.com/apps/me/maine/ag/reportingform)
Office of the Attorney General
Attorney General Aaron Frey

Re: Security Breach Notification

Dear Attorney General Frey:

We are writing on behalf of our client, Directions for Living (located at 1437 S Belcher Rd, Clearwater, FL 33764), to notify you of a data security incident involving four (4) Maine residents.[1]

Nature

On July 17, 2021, DFL discovered that it was the victim of a sophisticated ransomware attack that impacted its networks and servers. After discovering the incident, DFL worked to safely restore its systems and operations via viable backups. Further, DFL reported the incident to the FBI and engaged outside counsel and third-party forensic experts to conduct a thorough investigation of the incident, determine its scope, and assist in the remediation efforts.

DFL concluded its initial investigation on August 30, 2021, and determined that an unauthorized party gained access to its systems via a firewall vulnerability and encrypted some of its systems that contained protected health and other personal information. DFL has since remedied the vulnerability and secured its systems to the best of its ability.

Concurrently, DFL performed a comprehensive investigation to determine the nature of the impacted information and confirmed that the unauthorized individual(s) potentially obtained some protected health and other personal information. Further, on September 7, 2021, DFL confirmed the identity of the four (4) Maine residents.

However, as of now, we have no evidence indicating misuse of any of this information. Further, notification to individuals potentially affected by this incident is being performed out of an abundance of caution and pursuant to the organization's obligations under HIPAA and applicable state data breach notification laws.

The protected health and personal information potentially included first and last names, addresses, dates of birth, social security numbers, diagnostic codes used for billing purposes, claims and insurance information, name of health care provider, date of health care services, and certain other health information, but not any individual's electronic health record (DFL's electronic health record was never accessed or impacted by this event at any point).

[1] By providing this notice, Directions for Living does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Notice and Directions for Living's Response to the Event

On September 15, 2021, Directions for Living will mail a written notification to the potentially affected Maine residents, Maine Rev. Stat. Ann. Tit. 10, § 1346-49, in a substantially similar form as the enclosed letter (attached as Exhibit A).

Additionally, Directions for Living is providing these potentially impacted individuals the following:

- Free access to credit monitoring services for one year, through Cyberscout;
- Guidance on ways to protect against identity theft and fraud, including steps to report any suspected activities or events of identity theft or fraud to their credit card company and/or bank;
- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;
- A reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports; and
- Encouragement to contact the Federal Trade Commission and law enforcement to report attempted or actual identity theft and fraud.

Further, Directions for Living provided the notice to the three major credit reporting agencies along with the applicable government regulators, officials, and other Attorneys General (as necessary).

Finally, Directions for Living is working to implement any necessary additional safeguards, enhance and improve its policies and procedures related to data protection, improve its cybersecurity infrastructure, and further train its employees on best practices to minimize the likelihood of this type of incident occurring again.

Contact Information

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 832-8002 or email me at spollock@wtplaw.com.

Sincerely Yours,

Spencer S. Pollock, Esq., CIPP/US, CIPM

EXHIBIT A

Directions for Living
P.O. Box 3923
Syracuse, NY 13220

<First Name><Last Name>
<Address>
<City, State ZIP>

September 15, 2021

Re: Notice of Data Breach

Dear <First Name><Last Name>,

For nearly 40 years, Directions for Living has been a proud and trusted resource for those seeking a welcoming and compassionate provider of behavioral health services. We take this role, and our commitment to our community, very seriously.

As a part of that commitment, we place tremendous value on our clients' security and privacy. Unfortunately, we are writing to inform you that we recently became aware of a data privacy incident that may involve your personal information. Below, we have included steps we are taking toward resolution, and outlined services and recommendations for protecting your information and minimizing the impact of the incident, including complimentary identity monitoring and protection services. Enrolling in these services and following the recommendations provided will increase the likelihood your information remains protected. ***As of the date of this release, DFL has no evidence indicating misuse of any of your information. Notification to individuals potentially affected by this incident is being performed out of an abundance of caution and pursuant to the organization's obligations under the Health Insurance Portability and Accountability Act (HIPAA).***

We understand this type of situation can be stressful and raise a lot of questions. We have set up a dedicated helpline to help answer your questions, the details of which are below. In the meantime, here are the important details regarding the event and our response:

- On July 17, 2021, we discovered our servers may have been illegally accessed through the use of sophisticated ransomware, exposing the personal and protected health information of a portion of our current and former consumers.

- We promptly notified law enforcement and engaged outside legal counsel and third-party forensic experts to conduct a thorough investigation into the scope of the event and to assist with remediation efforts.

- The investigation concluded on August 30, 2021, at which point we began the process of notifying the potentially impacted individuals.

- After reviewing the potentially impacted protected health and personal information, DFL determined that it may include first and last names, addresses, dates of birth, social security numbers, diagnostic codes used for billing purposes, claims and insurance information, name of health care provider, date of health care services, and certain other health information, but not any individual's electronic health record. ***It is***

important to note that DFL's electronic health record was never accessed or impacted by this event at any point.

- DFL does not keep any client payment information on its servers. However, given the nature of the information that may have been impacted, we do recommend you remain vigilant by closely reviewing account statements and credit reports. Below (under "**Other Important Information**"), we have provided additional resources and tips to monitor this information and prevent identify theft. ***Again, we have no evidence that your information has been misused.***

- Further, in response to this incident, we are implementing additional cybersecurity safeguards and enhancing our cybersecurity policies, procedures, and protocols, as well as employee cybersecurity training.

- Finally, we are providing you with access to **Single Bureau Credit Monitoring*** services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft. These services will be provided by Cyberscout, a company specializing in fraud assistance and remediation services.
  To enroll in Credit Monitoring* services at no charge, please log on to **<URL>** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<access code>**
  In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

We have set up a dedicated toll-free helpline to help answer your questions. This can be reached at <Toll-Free Number> on Mondays through Fridays between 8:00 am to 8:00 pm Eastern time. In addition, individuals seeking to contact DFL directly may write to <DFL Address>.

Please know that your privacy is always our top priority, and we are working diligently to respond appropriately and continue to ensure that you are protected, and your information is safe with us.

Sincerely yours,

April Lott, LCSW
President & CEO

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 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.

OTHER IMPORTANT INFORMATION

Obtain and Monitor Your Credit Report. We recommend that you obtain a free copy of your credit report from each of the three nationwide credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 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 can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action

Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below to request a copy of your credit report or general identified above inquiries.

Equifax	**Experian**	**TransUnion**
(888) 766-0008	**(888) 397-3742 (800) 680-7289**	
P.O. Box 740256	P.O. Box 2104	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze (also known as a Credit Freeze). Following is general information about how to request a security freeze from the three credit reporting agencies. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. In addition, in some states, the agency cannot charge you to place, lift or remove a security freeze. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided above).

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	**Security Freeze & Fraud Victim Assistance Dept.**
Atlanta, GA 30348	Allen, TX 75013	P.O. Box 6790
https://www.freeze.equifax.com	www.experian.com/freeze	Fullerton, CA 92834
		https://freeze.transunion.com

Consider Placing a Fraud Alert on Your Credit Report. 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 twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three nationwide credit reporting agencies identified above. Additional information is available at https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Remain Vigilant, Review Your Account Statements and Notify Law Enforcement of Suspicious Activity. As a precautionary measure, we recommend that you remain vigilant by closely reviewing your account statements and credit reports. If you detect any suspicious activity on an account, we strongly advise that you promptly notify the financial institution or company that maintains the account. Further, you should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint or to contact the FTC, you can (1) send a letter to the *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

Take Advantage of Additional Free Resources on Identity Theft. We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf 0009_identitytheft_a_recovery_plan.pdf.

Maryland residents may wish to review the information the Attorney General, who can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, or visiting www.oag.state.md.us. **New Hampshire residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above. **New Mexico residents**, 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. **New York Residents**: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: *New York Attorney General's Office Bureau of Internet and Technology*, (212) 416-8433, https://ag.ny.gov/internet/resource-center and or NYS Department of State's Division of Consumer Protection, (800) 697-1220, https://www.dos.ny.gov/consumerprotection. **North Carolina residents** may wish to review the information provided by the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/identity-theft/, or by contacting the Attorney General by calling *1-877-566-7226* or emailing or by mailing a letter to the Attorney General at *North Carolina Attorney General's Office* 9001 Mail Service Center Raleigh, NC 27699. **Oregon Residents**: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877- 9392, www.doj.state.or.us. **West Virginia residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above.