September 21, 2023

Karen I. Bridges
312.706.3023 (Direct)
karen.bridges@wilsonelser.com

Via Online Portal:

Attorney General Aaron Frey
Office of the Attorney General
Attn: Security Breach Notification
Department of Professional & Financial Regulation
Bureau of Consumer Credit Protection
35 State House Station
Augusta, Maine 04333

Re: Cybersecurity Incident Involving Kannact, Inc.

Dear Attorney Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Kannact, Inc. ("Kannact"), an Oregon-based organization that works with various healthcare entities to provide healthcare collaboration solutions, located at 425 SW 2nd Ave, Suite 201, Albany, OR 97321, with respect to a cybersecurity incident that was first discovered by Kannact on March 13, 2023 (hereinafter, the "Incident"). Kannact takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of residents being notified, and the steps that Kannact has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals.

1. Nature of the Incident

On March 13, 2023, Kannact discovered that an unauthorized individual gained access to a limited portion of its system. Upon discovery of this Incident, Kannact promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. A preliminary review determined that the cause of the unauthorized access was a third party file transfer software. While the forensics investigation was ongoing, Kannact provided substitute notice pursuant to HIPAA on April 12, 2023 via Kannact's website and media release to the Wall Street Journal and USA Today. Kannact also published in the Oregonian.

On June 13, 2023 the forensic investigation concluded and found evidence that suggested an unauthorized individual compromised sensitive data from one of Kannact's third party file transfer solutions. There was no other unauthorized activity in Kannact's environment and no evidence of

any compromised sensitive personal information from any other systems in Kannact's environment. In sum, the scope of the incident was limited in nature, arising from a software vulnerability in Kannact's third party file transfer solution.

During the course of the forensic investigation, Kannact engaged a third party data mining vendor in order to identify the specific individuals and corresponding personal information potentially impacted associated with the third party file transfer solution. On May 19, 2023, Kannact received a preliminary list of covered entities whose members were potentially impacted, however, data mining did not provide an accurate list of individuals who were impacted. On June 12, 2023, Kannact received another list of covered entities and impacted individuals, but without sufficient information to fully identify the individual or assign them to a covered entity, and without all the information about what data was impacted for each individual. On July 7, 2023, Kannact received the final notification list from the third party data mining vendor; however, the list contained incomplete contact information for a significant amount of individuals.

As such, Kannact worked with the impacted Covered Entities throughout the data mining process to populate the incomplete contact information and determine whether to proceed with notification on behalf of the Covered Entities. This process remains ongoing, due to the number of Covered Entities involved, and an accurate total number of individuals impacted by this Incident has not yet been determined. However, on July 10, 2023, Kannact proceeded in notifying the first wave of individuals from Covered Entities that responded. The second wave of notification letters were mailed on August 14, 2023. The third wave of notification letters were mailed on August 23, 2023. The fourth wave of notification letters were mailed on August 28, 2023. The fifth wave of notification letters to the potentially impacted individuals were mailed on September 20, 2023. All individual notices were prepared pursuant to HIPAA.

It is possible that individuals' full name, address, date of birth, Social Security Number, health insurance information, and protected health information, including, but not limited to, medical diagnosis, treatment, pharmaceutical records, and Kannact ID may have been exposed as a result of this unauthorized activity. Please note not all data elements were potentially exposed for each individual.

2. Number of Maine residents affected.

A total of 284 Maine residents may have been potentially affected by this incident. Notification letters to these individuals were mailed on the following dates by first class mail: August 14, 2023; August 23, 2023; and September 20, 2023. A sample copy of the notification letter is included with this letter under **Exhibit A**.

Kannact is also providing notice on behalf of the following Covered Entities:

Covered Entity	**Number of Residents**
Washington County School District	1
Indian River County	2
Weber School District	1

Pathways	178
City of Dallas	1
Grand Prairie	1
Nuskin	1
Orthofix	4
Wellpath	93

3. Steps taken in response to the Incident.

Kannact is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, Kannact moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Specifically, Kannact engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, Kannact disabled access to the third party managed file transfer software, deactivated all related API keys, and is improving the patient data ingestion process.

Kannact also provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission. Kannact offered 12 months of complimentary credit monitoring and identity theft restoration services through IDX to individuals to help protect their identity.

4. Contact information

Kannact 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 karen.bridges@wilsonelser.com or (312) 706-3023.

Sincere Regards,

Wilson Elser Moskowitz Edelman and Dicker LLP

Karen Bridges

Karen I. Bridges

EXHIBIT A

Kannact
PO Box 480149
Niles, IL 60714

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/kannact

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Via First-Class Mail

<<Month>> <<Day>>, 2023

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

Kannact, Inc. ("Kannact") is partnered with <<Covered Entity>> as part of the employee benefits package to provide health coaching and assistance to <<Covered Entity>> employees who are enrolled in <<Covered Entity>>'s health insurance plan. To effectively help the individuals enrolled, Kannact has access to employee information who are enrolled in <<Covered Entity>>'s health insurance plan. We are writing to inform you of a data security incident that occurred with Kannact that resulted in unauthorized access to your personal information. Kannact sincerely regrets any inconvenience or concern that this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

What Happened?

On March 13, 2023, Kannact discovered that an unauthorized user gained access to its system. Upon discovery of this incident, Kannact promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. The preliminary findings determined that the cause of the unauthorized access was a third party file transfer software. While the forensics investigation was on going, Kannact provided substitute notice pursuant to HIPAA on April 12, 2023. Kannact engaged a third party data mining vendor to identify the covered entities involved, the specific individuals impacted, and the type of data that was in the file transfer software. On May 19, 2023, Kannact received a preliminary list of covered entities whose members were potentially impacted, however, data mining did not provide a full list of potentially impacted individuals or addresses for those they did identify. On June 12, 2023, Kannact received another list of covered entities and impacted individuals, but without sufficient information to fully identify the individual or assign them to a covered entity. Kannact has been working to obtain addresses to provide sufficient notice to individuals. On June 13, 2023, the forensic investigation completed by the third party cybersecurity firm confirmed that the cause of the unauthorized access to sensitive information was the third party file transfer software.

What Information Was Involved?

Based on the investigation, the following information related to you was subject to unauthorized access: <<Data Set>>.

What We Are Doing

Data privacy and security is among Kannact'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. Kannact has taken and will continue to take steps to mitigate the risk of future issues. Specifically, Kannact engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. Kannact also disabled access to a third party managed file transfer software, deactivated all related API keys, and is improving our patient data ingestion process.

In addition, we are providing you with access to **Single Bureau Credit Monitoring, CyberScan dark web monitoring, a $1,000,000 insurance reimbursement policy and fully managed identity theft recovery** services at no charge. These services provide you with alerts for <<12 / 24>> 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, we are 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 IDX, a ZeroFox Company, specializing in fraud assistance and remediation services. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

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 **https://response.idx.us/kannact** and follow the instructions provided. When prompted please provide the unique enrollment code provided above to receive services. In order for you to receive the monitoring services described above, you must enroll by October 10, 2023. The enrollment requires 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.

For More Information

If you have any questions or concerns not addressed in this letter, please call 1-888-566-0890 between the hours of 8:00 am to 8:00 pm Central Time, Monday through Friday (excluding U.S. national holidays).

Kannact 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,

Nandan Rao
Chief Operating Officer
Kannact 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.

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